資料37－3

# 国際連携の現状と課題

令和４年４月

サイバーセキュリティタスクフォース事務局

# 前々回タスクフォースの振り返り①



## 総務省におけるこれまでの取組（前々回タスクフォース資料抜粋）

### ○二国間の連携

・総務省が主催する各国とのICT分野の政策対話や外務省が主催するサイバー協議等において、我が国のサイバーセキュリティ政策等の積極的な発信や意見交換を実施。

### ○多国間の連携

・OECDの政策議論のほか、QUAD（日米豪印戦略対話）のサイバー上級会合や日ASEANサイバーセキュリティ政策会議等、多国間のセキュリティ関係の議論に積極的に参画。

### ○国際的なISAC間等連携

・サイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として、一般社団法人ICT-ISACと2019年に協力覚書を締結した米国IT-ISAC及びその関係機関との連携について、引き続き定期会合の開催等を通じて強化。また、米国に加えて他の国・地域等との連携も検討。

・ASEAN諸国を対象としたISP向け日ASEAN情報セキュリティワークショップを開催。また、ASEAN地域のISPとの情報共有体制を構築。

### ○開発途上国の能力構築支援

・ASEAN各国との協力関係を強化するため、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）において、CYDER等を通じて、ASEANのセキュリティ人材の育成支援を実施（2022年までに700名程度を目標。2021年12月現在734名が参加）。また、オンライン環境で受講可能なプログラムの拡充、有志国との第三者連携、国内企業により開発された演習の提供等を実施。

### ○国際標準化

・2016年7月にIoT推進コンソーシアムにおいて策定されたIoTセキュリティガイドラインの国際標準への反映等に向けて、ITU-T及びISO/IECにおけるIoTセキュリティに係る国際標準化の議論に積極的に貢献。

・「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、必要な調査や連携体制の強化の取組を実施。

# 前々回タスクフォースの振り返り②



**○国内企業のサイバーセキュリティ製品・ソリューションの国際展開支援**

・ASEAN諸国を中心に、国内企業のサイバーセキュリティ製品・ソリューションの海外への展開を支援するための実証事業等を実施。

**○国際的な情報共有等の推進**

・2021年に改定したスマートシティセキュリティガイドラインなどについて、国際連携の場で共有。

・DAEDALUSのアラート提供に関する有志国との試行的連携を実施。

## 前々回タスクフォースでお寄せいただいた意見（抜粋）

- ✓ 欧米のように政界とセキュリティ分野の架け橋となる人材を地域コミュニティから輩出するのは重要だと思うが、ASEAN地域での能力構築支援の取組には各国政府が選抜した人材が参加しており、地域コミュニティと分断されている。日本がリーダーシップを取り、多様な人材の募集を支援できるとよい。（篠田構成員）
- ✓ ISOではIoT推進コンソーシアムの成果を反映したIoTセキュリティプライバシーガイドラインが出来つつあるので、この場で議論できるとよい。（中尾構成員）
- ✓ ビジネスの海外展開は、特にアジアでは大変で実にならないが、継続して取り組まないといつまでも前進しないので、政府として進めていくことが重要。（鵜飼構成員）
- ✓ 一方で、国際連携全体について、経済安全保障の観点から戦略を練り直し、地域や領域を絞ることも必要。経済安全保障を議論する政府内の枠組みとのすり合わせも必要。（鵜飼構成員）

- **二国間連携**
- 多国間連携
- ISAC間連携
- 能力構築支援
- 国際標準化
- 海外展開支援

# 二国間連携



- 既存の枠組みを活用し、米国をはじめとするG7各国を中心に総務省のサイバーセキュリティ政策（IoTセキュリティ、５Gセキュリティ、能力構築支援等）に関する情報を発信。
- また、相手国のサイバーセキュリティ政策に関する情報を聴取、意見交換を行いながら、連携強化のための関係性構築を図る。

## 主な枠組み（総務省主催国際会議）

- インターネットエコノミーに関する日米政策協力対話
- グローバル・デジタル連結性パートナーシップ(GDCP)作業部会
- 日EU・ICT政策対話
- 日EU・ICT戦略ワークショップ

## その他の主な国際会議等

- 外務省が主催するサイバー協議・対話では、計13か国・地域との間で、年1回程度の頻度でサイバー空間に関する政府横断的な政策議論・対話を継続的に実施。
- 途上国地域を含むその他の二国間での対話の場においても、総務省の関連施策の紹介や民間情報共有活動に係る連携の促進等、具体的な協調関係を構築。

## 直近の主な取組

○ インターネットエコノミーに関する日米政策協力対話（第12回局長級会合）：2021年11月11日（木）・12日（金）
○ 日EU・ICT戦略ワークショップ（第12回）：2021年11月17日（木）
○ 第４回日エストニアサイバー協議：2021年12月22日（金）

- 二国間連携
- **多国間連携**
- ISAC間連携
- 能力構築支援
- 国際標準化
- 海外展開支援

# 多国間連携



➢ 多国間の枠組みであるITU-T、OECD等に積極的に参画し、サイバーセキュリティに関する政策的な協調や合意文書の作成等を実施している。

## ITU-T/SG17

- ITU（国際電気通信連合）では、国際標準化を担うTセクタにおいてSG（Study Group）ごとに国際標準となる勧告を議論。SG17は「セキュリティ」を担当。

## OECD/SDE

- 経済協力開発機構 （OECD：Organisation for Economic Co-operation and Development）のデジタル経済政策委員会（CDEP）に設けられているデジタル経済セキュリティ作業部会（SDE：Working Party on Security in the Digital Economy)において、サイバーセキュリティ政策に関する議論を実施。2021年１月より、総務省職員がSDE副議長を務めている。

※2023年にセキュリティ関係のOECDイベントである「グローバルフォーラム」を日本（総務省）が事務局とともに主催する予定。

## 日・ASEANサイバーセキュリティ政策会議

- 日本とASEAN諸国間の情報セキュリティ分野での連携・協力を進めるため、日本（NISC）主導で2009年2月に設けられた枠組み。
- 2015年2月に政策会議下に「ワーキンググループ（WG）」を立ち上げ、具体的な協力活動を推進。

# 日・ASEANサイバーセキュリティ政策会議



## 経緯・目的

- 日本とASEAN諸国間の情報セキュリティ分野での連携・協力を進めるため、日本（NISC）主導で2009年2月に「日・ASEAN情報セキュリティ政策会議」を立ち上げ、以降毎年１回ペースで開催。（2017年10月の政策会議で「日・ASEANサイバーセキュリティ政策会議」に改称。）
- ASEAN 10か国、ASEAN事務局、日本が参加。NISC、総務省、経産省が主催。
- 2013年9月に「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催。
- 2015年2月に政策会議下に「ワーキンググループ（WG）」を立ち上げ、「重要インフラ防護」、「サイバー演習」、「意識啓発」等をテーマとした協力活動を行っている。数次の体制変更を経て現在年に3回のWG会合を開催。

## 会議体

- **日・ASEANサイバーセキュリティ政策会議　（局長・審議官級）**
  - ✓ 情報セキュリティ分野におけるASEANとの協力枠組み等を議論・決定する。

  ※開催実績・予定：
  第１回(2009.2　東京)、第２回(2010.3　バンコク)、第３回(2011.3　東京)、第４回(2011.11　クアラルンプール)、第５回(2012.10　東京)、第６回(2013.10　マニラ)、第７回(2014.10　東京)、第８回(2015.10　ジャカルタ)、第９回(2016.10　東京)、第10回(2017.10 シンガポール)、第11回(2018.10 東京)、第12回(2019.10 バンコク)
  第13回(2020.10 オンライン)、第14回(2021.10 オンライン）、
  第15回（2022.10　東京（予定））

第12回日ASEANサイバーセキュリティ政策会議模様

- **日・ASEANサイバーセキュリティWG会議　（課長級）**
  - ✓ 政府機関の情報セキュリティ対策についての具体的な協力活動を推進する。

  ※直近の開催実績・予定：
  2020年：第1回(2020.2 シェムリアップ)、第2回(2020.6 オンライン)、第3回(2020.8 オンライン)
  2021年：第1回(2021.2 オンライン)、第2回(2021.6 オンライン)、第3回(2021.9 オンライン)
  2022年：第1回（2022.2　オンライン）、第2回（2022.6　オンライン（予定））、第3回（2022.8　インドネシア(予定)）

- 二国間連携
- 多国間連携
- **ISAC間連携**
- 能力構築支援
- 国際標準化
- 海外展開支援

# 日米のISAC連携の推進に関する取組



- 複雑化・高度化が進むサイバー空間の脅威に対応するために、官民での情報共有に加え、国際連携の強化が重要。
- 総務省では、サイバー脅威に対する国内通信インフラ事業者の対処能力向上を目的として、日米の情報通信分野ISAC(*)組織間における情報共有・連携を推進。

(*) ISACとは、Information Sharing and Analysis Center（情報共有分析センター）の略で、特定の産業界において、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに設立される組織。

## ■ 日米ISAC連携ワークショップのこれまでの開催実績

- 2016年11月： 日米ISAC関係者による初めての国際連携会合を開催。日米のサイバー脅威動向や取組状況等を意見交換。
- 2017年11月： 第2回会合を開催。米国IT-ISACの保有するサイバー脅威関連情報のICT-ISACへの提供等について合意。
- 2019年２月： 第3回会合を開催。各ISACが情報共有を推進する上での懸念事項を共有し、その解決策等を議論。併せて、公開シンポジウムも開催。
- 2019年11月： 第4回会合を開催。ICT-ISACと米国IT-ISACが協力に係る覚書に署名。
  (1) サイバー脅威とインシデント情報の共有
  (2) 脅威情報の共有を自動化する仕組みの構築に向けた協力
  (3) 両ISAC会員企業間での協力の促進
- 2020年１月： 2020年1月のPTC（太平洋電気通信協議会）においてフォローアップ会合を実施。
- 2021年４月： 第5回会合をリモートで開催。
- 2022年２月： 第6回会合をリモートで開催。


ICT-ISACと米国IT-ISACによる
覚書署名式の様子（2019年11月）


第4回公開シンポジウム
パネルディスカッション（2019年11月）

# 米国以外の地域（EU等）との情報共有活動の促進



- 民間情報共有組織におけるサイバーセキュリティ上の脅威情報や脆弱性情報の共有活動の一層の高度化等を図る観点から、米国以外の国・地域（EU等）との国際連携についても推進中。
- 連携先として、ICT分野の民間情報共有組織が既に存在し、又は設立されつつある国・地域を選択し総務省が相手国・地域の関係省庁を通じて調整を行っているところ。

## 目的

- 日本の民間情報共有組織における情報共有活動の高度化等に資する。
- 連携相手国との間でのサイバーセキュリティに関する協力関係の強化に資する。

## これまでの主な取組

- 総務省が、EU等の関係機関に呼びかけ、官民参加型のワークショップを主催。先進的な取組ないし独自の取組を行っている海外のICT分野の民間情報共有組織と日本のICT-ISACとの間でのベストプラクティスの交換等による連携促進を図っている。

-日EU International Workshop on Cybersecurity

- 開催日：2021年９月14日（オンライン形式）
- 出席者：日本側：総務省、NICT、ICT-ISAC、金融ISAC
  EU側　：DG-CONNECT、ENISA、FI-ISAC（金融ISAC）

-日米EU 意見交換会

- 開催日：2022年3月28日（オンライン形式）
- 出席者：日本側：総務省、ICT-ISAC
  EU側　：DG-CONNECT、EU・TLD-ISAC、PISAX、ETIS
  米国側：Comm-ISAC、IT-ISAC

# ISP向け日ASEAN情報セキュリティワークショップ



## 経緯・目的

- 日ASEAN情報セキュリティ政策会議（2010年3月）の結果を受け、総務省の主催により2011年1月に第1回を開催。基本的に年1回の頻度で開催しており、直近では2021年1月に第11回を開催。
- 日本とASEAN各国のISP事業者等におけるサイバーセキュリティ分野の取組状況の共有、意見交換及び人的ネットワークの維持・強化を目的としている。

## 開催実績・予定

| # | 開催時期 | 開催場所 |
|---|---|---|
| 第1回 | 2011年01月 | 日本（東京） |
| 第2回 | 2012年03月 | 日本（東京） |
| 第3回 | 2013年02月 | タイ（バンコク） |
| 第4回 | 2013年08月 | 日本（東京） |
| 第5回 | 2014年10月 | フィリピン（マニラ） |
| 第6回 | 2015年12月 | 日本（東京） |
| 第7回 | 2016年12月 | タイ（バンコク） |
| 第8回 | 2018年02月 | 日本（東京） |
| 第9回 | 2019年01月 | シンガポール |
| 第10回 | 2019年12月 | タイ（バンコク） |
| 第11回 | 2021年1月 | リモート |
| 第12回 | 2022年1月 | リモート |

第10回ワークショップ模様


第11回ワークショップ(オンライン開催)の模様

- 二国間連携
- 多国間連携
- ISAC間連携
- **能力構築支援**
- 国際標準化
- 海外展開支援

# AJCCBCにおけるASEANのセキュリティ人材育成



- AJCCBC（日ASEANサイバーセキュリティ能力構築センター）は、JAIF（日・ASEAN統合基金）を活用した、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人材育成プロジェクト。
- 2017年12月の日ASEAN情報通信大臣会合にて総務省が議論をリードし、タイのETDA（電子取引開発庁）がセンターを運用することで合意。2018年９月にセンター開所。

## センターの主な活動内容

1. **サイバーセキュリティ演習**
   ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習を実施（年6回程度）
   - ✓ 実践的サイバー防御演習（CYDER） ※CYDER: Cyber Defense Exercise with Recurrence
   - ✓ デジタルフォレンジック演習
   - ✓ マルウェア解析演習

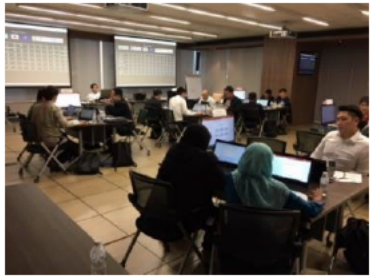
   ※2021年度は試行的に公開情報等分析（スレットハンティング）演習を実施するとともに、SOCアナリスト向け演習も実施予定

2. **Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）**
   ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競うCTF形式の大会の開催（年１回）

   ※CTFとは、Capture The Flagの略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式の競技

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

日ASEAN情報通信大臣会合（2017年12月）



サイバーセキュリティ演習

## 研修開催実績

- 2018年9月のセンター開所以来、約2ヶ月に1回のサイバーセキュリティ演習と年1回のCyber SEA Gameを開催。
- 2022年3月時点で計787名が参加。（目標である4年間で700人程度の育成を達成）
- 2022年3月に有志国であるスイスよりセキュアなプログラミング方法について学ぶための研修を実施

**今後、センターの活動に関する有志国等（アメリカ、イギリス、スイス等）との連携を強化し、研修プログラムの提供・実施を予定**

- 二国間連携
- 多国間連携
- ISAC間連携
- 能力構築支援
- **国際標準化**
- 海外展開支援

# ITU-T SG17会合 研究課題



- ITU SG17では通信分野におけるSecurity標準を担当している。専門家による助言の下、日本提案の勧告への支援と、懸念国からの提案への対処を行っている。
- IoT推進コンソーシアム・総務省・経済産業省が公表した「IoTセキュリティガイドラインver1.0（2016年7月）」の勧告化に向けて議論が継続中。

| 課題番号 | 研究課題のタイトル |
|---|---|
| 1/17 | セキュリティ標準化戦略と調整 |
| 2/17 | セキュリティアーキテクチャとネットワークセキュリティ |
| 3/17 | 電気通信情報セキュリティ管理とセキュリティサービス |
| 4/17 | サイバーセキュリティと迷惑メール対策 |
| 6/17 | 電気通信サービスとモノのインターネット（IoT）のセキュリティ |
| 7/17 | 安全なアプリケーションサービス |
| 8/17 | クラウドコンピューティングとビッグデータ・インフラストラクチャ・セキュリティ |
| 10/17 | ID 管理とテレバイオメトリクス・アーキテクチャ及びメカニズム |
| 11/17 | セキュアなアプリケーションを支える汎用技術（ディレクトリ、PKI、形式言語、オブジェクト識別子など） |
| 13/17 | 高度道路交通システム（ITS）セキュリティ |
| 14/17 | 分散型台帳技術（DLT）のセキュリティ |
| 15/17 | 量子ベースのセキュリティを含む新技術のための/によるセキュリティ |

# IoTセキュリティガイドラインの国際標準化



➢ IoT推進コンソーシアム・総務省・経済産業省が公表した「IoTセキュリティガイドラインver1.0（2016年7月）」の国際標準化に向け、ITU-T及びISO/IECにおける議論を継続中。

IoT Acceleration Consortium

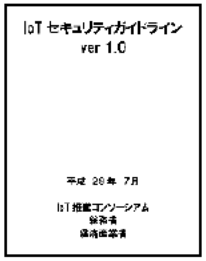
総務省　経済産業省

ITU-T及びISO/IECに対して
国際標準化に向けた検討を提案

ITU

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

○2016年7月、IoT推進コンソーシアム・総務省・経済産業省により、「IoTセキュリティガイドラインver1.0」を公表




（主な標準化項目）
・IoTシステムのステークホルダー
・IoTシステムに係るリスク分析
・IoT機器のライフサイクル
・適切なセキュリティ管理手順　等

○2018年4月以降継続的にISO/IEC JTC1 SC27において議論されていた、本ガイドラインをベースとしたIoTセキュリティ規格案（ISO/IEC 27400）が、国際規格原案として承認され、現在最終勧告案化に向けた準備が行われている。

○2018年9月、ITU-T SG17において、本ガイドラインをベースとして、IoTシステムのためのセキュリティ管理策に関する文書が勧告草案（X.sc-IoT）として承認され、議論を継続中。

- 二国間連携
- 多国間連携
- ISAC間連携
- 能力構築支援
- 国際標準化
- **海外展開支援**

# サイバーセキュリティソリューションの海外展開



## 実証事業概要

- 日本企業のサイバーセキュリティソリューション・製品等をASEAN諸国等に展開することを目的とした実証事業等を実施。
- 平成30年度事業：
  - ✓ セキュリティ対策に課題を抱えるASEAN諸国において、導入・運用が簡便かつ低コストであり、セキュリティ対策上の効果も高い技術の一つであるSD-WANを利用したセキュリティ共通基盤の導入効果を調査。
  - ✓ クアラルンプール大学内の施設である「UniKL-NEC SDx Centre of Excellence」が設立された。本施設のコア技術の提供をNECが受注。
- 令和元年度事業：
  - ✓ 前年度事業を契機に導入されたUniKLのSD-WANセキュリティ共通基盤を活用し、アノマリー型エンドポイントセキュリティ製品Yaraiと連携させた標的型攻撃対策ソリューションの導入効果を調査。
- 令和2年度事業：
  - ✓ マレーシア学術機関と連携し、 BYOD端末の本人認証の強化及び本人認証に基づくネットワークアクセスポリシーとの自動連携による日本発のセキュリティ対策ソリューションの実証事業実施。
- 令和3年度事業：
  - ✓ ベトナム学術機関と連携し、中小企業のセキュアなファイル授受によるセキュリティ対策ソリューションによる日本発のセキュリティ対策ソリューションの実証事業を実施。


センター設立の記念セレモニー（平成31年3月）
（中央はクアラルンプール大学学長）

実証事業中間報告会（令和元年年12月）

## 対外活動・受賞歴

- **PERISA ‘19 【シルバー受賞】、及び、PECIPTA '19 【シルバー受賞】**
  - ✓ マレーシア教育省及びマレーシア財閥MARAグループ主催の技術イノベーションコンペティションにて、本事業を含むセキュリティソリューションの紹介を行い、シルバー受賞。
  - ✓ マレーシア教育省及び高等教育機関であるInstitution of Higher Learning主催の国際展示会においても同様に本事業の紹介を行い、シルバー受賞。
- **MEF 3.0 Proof of Concept Showcase ’19 【SD-WAN Implementation部門アワード受賞】**
  - ✓ ネットワーク技術の標準団体であるMEF(Metro Ethernet Forum)主催のShowcaseにて、本事業で用いたSD-WANセキュリティ共通基盤のデモ展示及び紹介を行い、SD-WAN Implementation部門アワード受賞。
- **NACSA-MIC Webinar for ASEAN “Cybersecurity in the New Normal”（2021年度）**
  - ✓ マレーシア国家サイバーセキュリティ局（NACSA）とウェビナーを共催し、産学官から数百名の参加を得て、両国企業による最新のサイバー脅威や技術動向やR2年度の実証について紹介。


PERISA/PECIPTA シルバー受賞


MEFアワード受賞

# 論点



## 国際連携

○ 現在実施している二国間・多国間の国際的な官民連携をどのように発展させていくべきか。

○「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」（2021年12月14日サイバーセキュリティ戦略本部決定）を踏まえ、総務省としてASEAN地域やインド太平洋地域における能力構築支援をどのように推進すべきか。

○ 国内企業のサイバーセキュリティ製品・ソリューションの国際展開を支援していくうえで、どのような領域・地域に注力していくべきか。