資料29－４

# サイバーセキュリティ分野における国際連携について

サイバーセキュリティタスクフォース事務局

令和３年３月９日

# サイバーセキュリティ分野における国際連携の状況（全体概要）

■ 現在、総務省（サイバーセキュリティ統括官室）では、サイバーセキュリティに関する**二国間・多国間・官民の連携**や対**ASEAN諸国を中心とする能力構築支援**の取組を実施するとともに、**ISACやISP間等の民間の国際連携を促進**している。

## ①二国間・多国間連携

**総務省のサイバーセキュリティ政策について、積極的な対外発信と連携強化を推進**

**○二国間連携**
- インターネットエコノミーに関する日米政策協力対話
- 日EU・ICT政策対話・戦略ワークショップ
- その他、豪、中韓、英、仏を含む13か国等とのサイバー協議
- イスラエルの国家サイバー総局との間で協力覚書を締結　等

**○多国間連携**
- ITU-T SG17 等（標準化活動）

**○官民連携**
-Charter of Trust 等


石田総務大臣とベンアリ駐日イスラエル大使による覚書署名式（2018年11月）

## ②民間組織の国際連携の推進

**○ ISP向け日ASEAN情報セキュリティワークショップ**

日本とASEAN各国のISP事業者等との情報共有等の推進

**○ 日米ISAC連携ワークショップ**

日米の情報通信分野ISAC間における情報共有の推進。ICT-ISACと米国IT-ISACは、2019年11月に協力覚書を締結。


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

## ③能力構築支援

**○ 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）**

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

日・ASEAN統合基金（JAIF）を活用したASEAN域内のセキュリティ人材育成（４年間で700人程度を育成する目標）の拠点となるセンターで、2018年９月にタイで開所。ASEAN域内で高い評価を得ている。

**■ 研修プログラムの概要**

1. サイバーセキュリティ演習

政府機関や重要インフラ事業者等に対し、実践的サイバー防御演習（CYDER）等のプログラムを実施（年6回程度）

2. Cyber SEA Game

若手技術者・学生がサイバー攻撃対処能力を競う大会の開催（年１回）

**■ 活動内容のオンライン化**

新型コロナウイルス感染症拡大に伴う移動制限等を受け、上記研修プログラムのオンライン化を進めるとともに、①自己学習教材コース、②実践的解析演習コースのオンライン提供を開始。

**■ 第三者との連携を通じた活動内容の拡充**

欧米や国際機関等に対して、研修プログラムや講師の提供を募る予定。研修内容の拡充による日本とASESAN諸国との連携の深化に加え、日本と欧米等との連携の強化及び信頼醸成を図る。

# 1.1 二国間連携（既存の取組の紹介）

■ 現在、総務省が主催する各国とのICTに関する政策対話や外務省が主催するサイバー協議等において、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、スマートシティセキュリティ等）について発信する一方、相手国における主要なサイバーセキュリティ政策に関する説明を聴取しつつ、意見交換を行いながら、相手国政府との間での信頼醸成を推進。

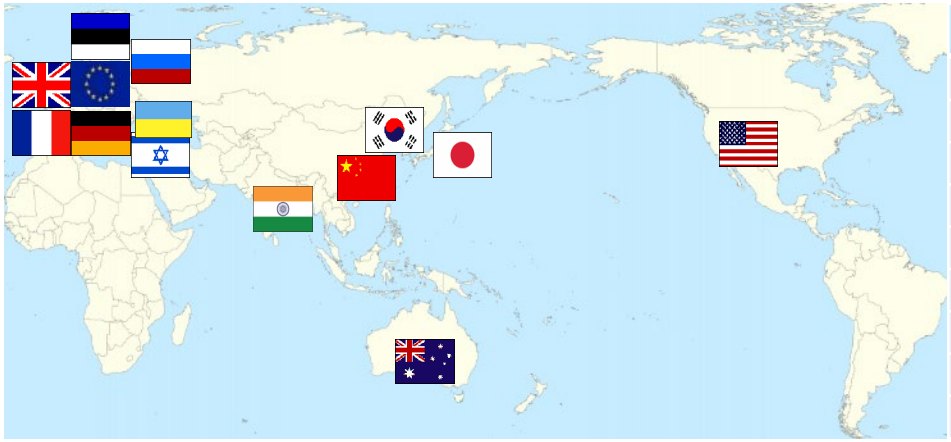
## 総務省が主催する主な国際会議

- 米国との「インターネットエコノミーに関する日米政策協力対話」、EUとの「日EU・ICT政策対話」及び「日EU・ICT戦略ワークショップ」等の二国間対話の場において、サイバーセキュリティに係る政策に関する意見交換を実施。
- 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。また、主要国の在京大使館職員等とも個別に意見交換等を実施。

## その他の主な国際会議

- NISC、総務省及び経産省が主催する「日・ASEANサイバーセキュリティ政策会議」では、ASEANとの協力枠組み等の議論・決定を行い、その下のWGでは、「重要インフラ防護」、「サイバー演習」、「意識啓発」等をテーマに具体的な協力活動を推進。
（2009年に日・ASEASN情報セキュリティ政策会議が設立され、2017年に現在の名称に改称された。）
- 外務省が主催するサイバー協議では、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を継続的に実施。

（参考）サイバー協議の開催実績



| | 英 | 印 | 米 | EU | 中・韓 | イスラエル | 仏 | エストニア | 豪 | 露 | 独 | ウクライナ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2012年 | ○ | ○ | | | | | | | | | | |
| 2013年 | | | ○ | | | | | | | | | |
| 2014年 | ○ | | ○ | ○ | ○ | ○ | ○ | ○ | | | | |
| 2015年 | | | ○ | | ○ | | | ○ | ○ | ○ | | |
| 2016年 | ○ | | ○ | | ○* | ○ | ○ | | ○ | ○ | ○ | ○ |
| 2017年 | | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | | | |
| 2018年 | ○ | | ○ | | | ○ | ○ | | | | | |
| 2019年 | | ○ | ○ | ○ | ○ | | ○ | | ○ | ○ | | |
| 2020年 | ○ | | | | ○ | | | | | | | ○ |

*2016年は韓国との間での二国間協議を開催

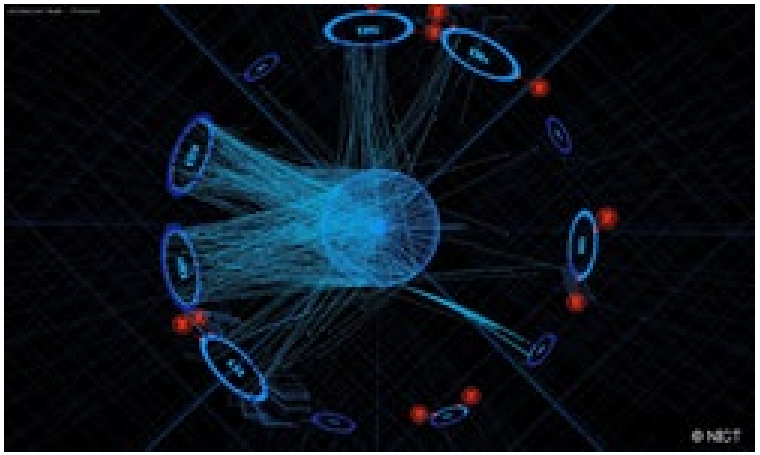
# 1.2 二国間連携（既存の取組 例:DAEDALUSの国際展開）

■ 2013年9月に開催された「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」において発足したプロジェクト「JASPER(Japan-ASEAN Security Partnership)」により、ASEAN諸国に対して、DAEDALUS*によるアラートを提供し、サイバー空間における攻撃の実態把握に資するとともに、ASEAN諸国のネットワークのモニタリング能力等の向上に寄与。

* DAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）とは、情報通信研究機構（NICT）が運用している、大規模ダークネット観測網を用いて、組織内から送出される異常な通信を検知し、当該組織に対して迅速にアラートを送信するシステム。

## DEADALUS

観測対象の組織について、組織内のマルウェアによる感染活動、組織内から組織外への感染活動、組織外の機関等が受けているDoS攻撃の跳ね返り（バックスキャッタ）等をダークネットで観測し、当該組織へ迅速にアラートを送信する。



DAEDALUSの可視化エンジン

## JASPERを通じたDAEDALUS提供国

JASPERによるマルウェア感染警告についての技術協力としてDAEDALUSによるアラートを提供。

- ミャンマー　：2013年10月～
- ラオス　：2013年11月～
- インドネシア　：2013年11月～
- フィリピン　：2013年12月～
- マレーシア　：2014年 3月～
- タイ　：2016年 4月～

ASEANにおけるサイバー脅威認識の共有、情報交換のための基盤として活用

（参考）https://www.nict.go.jp/out-promotion/other/case-studies/itenweb/DAEDALUS.html

# 2.1 民間情報共有組織間の国際連携の促進（既存の取組①）

- 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は、民間情報共有組織間での情報共有や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・連携を促進。

* 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。あわせて、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３月： 第5回会合をオンラインで開催予定。


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）

# 2.1 民間情報共有組織間の国際連携の促進（既存の取組②）

■ ASEAN地域に対しては、ISP間の国際連携を促進するために、「ISP向け日ASEAN情報セキュリティワークショップ」を開催し、日本・ASEAN諸国間のサイバーセキュリティ上の脅威への対応に関するベストプラクティスの共有に係る連携や人的ネットワークの構築・強化等を促進。

## 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、2011年1月に第1回ISP向け日ASEAN情報セキュリティワークショップを開催。同ワークショップは、基本的に年1回の頻度で開催。
- 日本及び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、人的ネットワークの構築・強化等を目的として、総務省が主催。

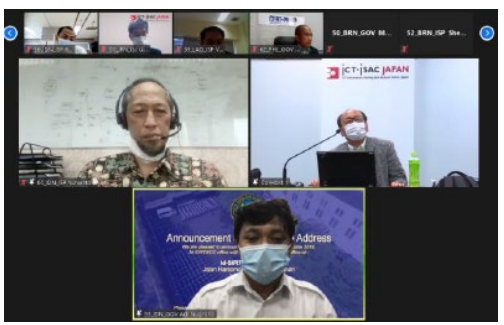
## 開催実績

- 2021年1月、第11回ワークショップを初のオンライン開催。実施効率を落とさないようにするため、オンライン上のプラットフォーム（Slack）を用いた情報共有体制を構築し、ワークショップの開催に先立って議論を深め、信頼の醸成を図った。

| | 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） |

| | 開催時期 | 開催場所 |
|---|---|---|
| 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 | オンライン |
| | ： | |

第10回ワークショップの模様



第11回ワークショップ(オンライン開催)の模様

# 3. 官民連携（例：Charter of Trustへの参画）

■ サイバーセキュリティの確保には、官民及び国境の壁を超えた連携が重要。

■ サプライチェーンリスク対策を含むサイバーセキュリティ確保のための民間主導の情報共有組織に参画し、最新のサイバーセキュリティ政策の発信及び諸外国の企業における取組等の情報収集を行い、国際的な官民間での信頼醸成を図る。

**主な取組**

- 総務省は、2021年１月、欧州の民間企業が主導するCharter of Trust (CoT)*の準メンバー（Associated Partner）となり、その集まりであるAssociated Partners Forum (APF)に参画。
- 今後、この枠組みを通じて、関係政策の国際的な発信や官民の連携チャネルの一層の拡大を図る。
- これまでの主な活動実績は以下のとおり。
  - Charter of Trust Tokyo Roadshow （2020年10月13日）
    総務省と海外民間企業・学術機関との間でサイバーセキュリティの強化に向けた議論を実施。
    IBM、Siemens、RSIS(シンガポールの高度学術機関・シンクタンク)、NTT、三菱重工等が参加。
  - Charter of Trust Virtual Collaboration Week（2021年１月25日～２月３日）
    総務省の政策紹介及び海外関係機関との間での意見交換を実施。
    NTT、三菱重工のほか、CoTメンバーとしてSiemens等の欧州の製造業関連企業が参加。準メンバーとして欧州委員会、独外務省、加サイバーセンター等が参加。

* Charter of Trustは、2018年2月にミュンヘン安全保障会議の場でSiemens主導により設立された業界横断的なサイバーセキュリティに関する情報共有・施策推進のための民間組織。現在、欧・米・アジアの産業界から17社・団体が参加。日本からはNTT、三菱重工が参加。
参加企業は自社や自産業のサプライチェーンひいては社会全体のサイバーセキュリティ強化を目的として、10の原則（「サイバー及びITセキュリティのオーナシップ」「デジタル・サプライチェーン全体を通した責任」「セキュリティ・バイ・デフォルト」「利用者中心」「イノベーションと共同作業による創造」「教育」「重要インフラ及びソリューションの認定」「透明性と対応」「規制枠組み」及び「共同イニシアティブ」から構成される）の策定とその具体化のための国際的な連携に取り組む。

# 4.1 能力構築支援（AJCCBCにおける活動）

■ ASEAN地域に対する能力構築支援は、同地域を踏み台とした日本へのサイバー攻撃の低減に結びつくことやその地政学的位置づけの観点から重要である。

■ 「日ASEANサイバーセキュリティ能力構築センター（AJCCBC）」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であり、総務省は、本センターにおける運営委員会への参画や演習の提供等を実施。

## 取組概要

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

- 2017年12月の日ASEAN情報通信大臣会合（※1）において、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。４年間で約700名の技術者を訓練することを目標として、2018年９月にバンコクにセンター開所。
- 活動開始後、毎回定員に近い研修への参加申込があり、日本の支援について高く評価されている（※2）。

（※1）2020年より日ASEANデジタル大臣会合に名称変更。
（※2）2019年11月の第14回日ASEAN情報通信大臣会合では，10か国中６か国がAJCCBC支援への感謝の意を表明。


日ASEAN情報通信大臣会合（2017年12月）

## センターの主な活動内容

**1. サイバーセキュリティ演習**

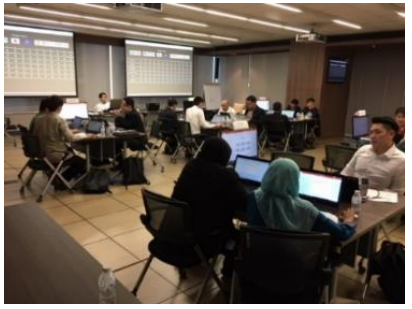
ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習を実施（年6回程度）

- ✓ 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

**2. Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）**

ASEAN各国からの若手技術者等がサイバー攻撃対処能力を競うCTF形式の大会を開催（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


サイバーセキュリティ演習