50th Year of ASEAN-Japan Friendship and Cooperation

日ASEANサイバーセキュリティの
これまでとこれから

日ASEAN
サイバーセキュリティ協力成果レポート

IC-AJCC 2023

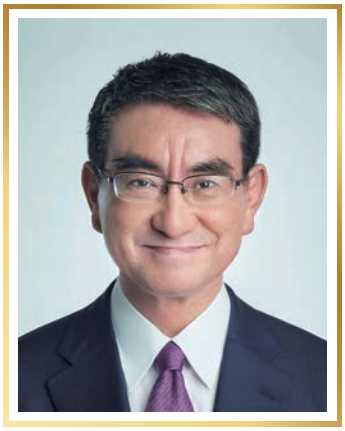
International Conference on ASEAN-JAPAN Cybersecurity Community

50th Year of ASEAN-Japan Friendship and Cooperation

ASEAN・JAPAN Cybersecurity Cooperation

NISC

大臣からのメッセージ



河野 太郎

（2023年9月13日時点）デジタル大臣、デジタル行財政改革担当、デジタル田園都市国家構想担当、行政改革担当、国家公務員制度担当、内閣府特命担当大臣（規制改革）

日頃から、日ASEAN友好協力にご尽力いただき感謝申し上げます。

2023年は、日本とASEANの友好協力50周年を迎える節目となる年です。これを記念し2023年10月5日及び6日に明治記念館において、記念イベント「日ASEANサイバーセキュリティ官民共同フォーラム」を開催しました。

半世紀にわたり日本とASEANの関係は目覚ましい発展を遂げ、アジア太平洋地域の平和と安定、発展と繁栄のために緊密な協力関係を築いてきました。

昨今のデジタル時代において、サイバーセキュリティの脅威はますます高度化し、広がっています。政府、組織、そして個人は、ハッキング、データ漏洩、ランサムウェア攻撃など、さまざまなサイバーリスクに直面しています。

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するためには、サイバー安全保障分野での対応能力を向上させることが必要です。このため、ASEAN加盟国と日本との間での情報の共有、能力構築支援等を含めた多様な連携・協力を進めることは非常に重要です。

日本政府としても、引き続き、ASEAN各国の皆様と連携し、「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定に貢献していきたいと考えていますので、ご協力いただければ幸いです。

「日ASEANサイバーセキュリティ官民共同フォーラム」を通して、日本とASEAN加盟国の国際協力活動がより一層進展することを期待しております。

功労者からのメッセージ

電子取引開発機構 政策・規格センター 専門官

Thongchai Sangsiri

ASEANと日本のサイバーセキュリティにおける協力は、ASEAN加盟国のサイバーセキュリティを強化し、地域内での安全なデジタル環境を推進するために重要な役割を果たしています。2023年9月の日ASEAN包括的・戦略的パートナーシップ設立の共同声明は、ASEANと日本のパートナーシップをさらに強化するでしょう。

インドネシア大学 IdCARE
（インドネシア・サイバー・アウェアネス・アンド・レジリエンス・センター）
共同設立者兼会長

Muhammad Salman

ASEANのサイバーセキュリティ・コミュニティへの日本の継続的な支援に心から感謝いたします。サイバーセキュリティ能力の向上、知識の共有、その他の取り組みにおいて、日本とのパートナーシップは強固なものとなりました。今後も日ASEAN協力のプラットフォームのもと、安全でクリーンかつ、信頼性の高いサイバースペースを構築できるよう、手を取り合って協力しあえることを願います。

BruCERT および CWC 代表
サイバーセキュリティブルネイ

Haji Mas Zuraime Haji Abdul Hamid

日ASEANサイバーセキュリティ協力における共同の努力が評価され、このような名誉ある賞をいただいたことを誠に光栄に存じます。この成果は、日ASEAN協力関係者全員の献身的で熱意ある取り組み、そして日本政府の貴重な支援がなくては成し得なかったものです。これからも共にデジタルの未来を確かなものにしていきましょう。

武蔵野大学国際総合研究所フェロー・客員教授
東京大学公共政策大学院 アドバイザー

林 良造

約15年前に手探りで始めた日ASEANサイバーセキュリティ政策会合が、ここまで深さと広がりを持った会合として定着するまでには国を超えた多くの人の貢献がありました。中でも特別の感謝を山口英元奈良先端技術大学院教にささげたいと思います。山口教授は早くからインターネットの重層的な十全性の重要さを認識しNISCの初代情報セキュリティ補佐官としてこの会合の設立に情熱をそそがれるとともに、自らアジア、アフリカと世界を飛び回り各地のNational CSIRTの設立をけん引されてきました。不幸にして難病に倒れられましたが、改めてこの会合がここまで育ったことをご報告します。

日ASEANサイバーセキュリティ会議の歩み

2009-2023

◆ 日ASEAN情報セキュリティ政策会議を立ち上げ

2009

〈２月〉
第１回情報セキュリティ政策会議（東京）
〈10月〉
第１回ワークショップ（東京）


第１回政策会議

2010

〈３月〉
第２回情報セキュリティ政策会議（バンコク）
〈10月〉
第２回ワークショップ（ハノイ）


第２回政策会議

2011

〈３月〉第３回情報セキュリティ政策会議（東京）
〈11月〉第４回情報セキュリティ政策会議
（クアラルンプール）


第３回政策会議

◆ 共同意識啓発を開始

2012

〈10月〉
第５回情報セキュリティ政策会議（東京）


第５回政策会議

2013

〈９月〉サイバーセキュリティ閣僚政策会議
（東京）
〈10月〉第６回情報セキュリティ政策会議
（マニラ）


第６回政策会議

2014

〈10月〉
第７回情報セキュリティ政策会議（東京）


第７回政策会議

2015

〈10月〉
第８回情報セキュリティ政策会議
（ジャカルタ）


第８回政策会議

2016

〈10月〉
第９回情報セキュリティ政策会議（東京）

リモートサイバー演習・机上演習
（ASEAN加盟国と日本との
サイバー連携強化も視野に
演習を実施）

2017

〈10月〉
日ASEANサイバーセキュリティ政策会議
に改称

〈10月〉
第10回日ASEANサイバーセキュリティ
政策会議（シンガポール）


第10回政策会議

2018

〈10月〉
第11回日ASEANサイバーセキュリティ
政策会議（東京）

相互通知プログラムの活動を開始

2019

〈10月〉
第12回日ASEANサイバーセキュリティ
政策会議（バンコク）

2020

〈11月〉
第13回日ASEANサイバーセキュリティ
政策会議（オンライン）

「モバイル端末における
サイバーセキュリティ」をテーマに、
各国でインフォグラフィックを作成し、
E-booklet を作成

◆ 各国で意識啓発に活用

2021

〈10月〉
第14回日ASEANサイバーセキュリティ
政策会議（オンライン）


第15回政策会議

2022

〈10月〉
第15回日ASEANサイバーセキュリティ政策会議（東京）

各国での産官学連携事例について共有 - GLOBIS大学院大学の
“MBA for Cybersecurity”科目が初開講


IC-AJCC 2023

2023

日ASEANサイバーセキュリティ官民共同
フォーラム（東京）IC-AJCC 2023

日ASEANサイバーセキュリティ協力関連の取組例

日ASEANサイバーセキュリティ官民共同フォーラム

令和5年10月5日(木)から6日(金)まで、明治記念館にて、日ASEAN友好協力50周年を記念し、サイバーセキュリティ分野における我が国とASEAN諸国との国際的な連携・取組を強化することを目的とし、「日ASEANサイバーセキュリティ官民共同フォーラム」を開催。内閣サイバーセキュリティセンターでは、関係省庁とも連携しつつ、今後も日ASEANの協力関係の強化に取り組む。

河野大臣挨拶


MoU締結

功労者表彰


集合写真

共同意識啓発

2012年から開始。
2021年、「モバイル端末におけるサイバーセキュリティ」をテーマに、各国でインフォグラフィックを作成し、E-booklletを作成。(リード国:ブルネイ・シンガポール)
2022年、各国で意識啓発に活用。(UNIDIR(国連軍縮研究所)のCyber Policy Portalにも掲載)


NISC公式キャラクター
セキュちゃん


表紙


ブルネイ


カンボジア


インドネシア

日本


ラオス


マレーシア

ミャンマー


フィリピン


シンガポール


タイ


ベトナム

リモートサイバー演習
(RCX:Remote Cyber Exercise)

毎年6月にオンラインで実施。疑似的なインシデント対処のシナリオを組み、各国のCERT体制とオンラインチャット(Mattermost)を使用して情報連絡。

ランサムウェア等の近年のサイバー攻撃を例題として、インシデント認知・情報展開・分析・対処等の一連のインシデントハンドリングを疑似した訓練を実施。

机上演習
(TTX:Table Top Exercise)

毎年8月に対面で実施(2020年は中止、2021年はオンラインで実施)。各国の政策立案担当者と、サイバーセキュリティに関する機微なテーマについて議論し、知見を共有する。

DX with Cybersecurityやサイバー攻撃等、テーマを決めて、各国政府の取組状況等を共有し、政策立案に役立てる。

CIIPワークショップ

2015年から活動開始。
重要情報インフラ防護(CIIP)に関して、各国の活動状況や最新の知見を共有するワークショップを開催。

JICAの取組

サイバーセキュリティ能力強化を支援

カンボジア向け技術協力プロジェクト討議議事録の署名

国際協力機構(JICA)は、11月29日プノンペン都にて、カンボジア王国政府との間で技術協力プロジェクト「サイバーセキュリティ能力向上プロジェクト」に関する討議議事録(Record of Discussions:R/D)に署名。

カンボジアでは、郵政通信省のICTセキュリティ局に国家CSIRT(注)であるCamCERT(Cambodia Computer Emergency Response Team)が配置されています。本案件は、日々高度化するサイバー攻撃等に対応するため、ICTセキュリティ局を中心にサイバーセキュリティ能力向上支援を行い、将来的にカンボジア全体におけるデジタル社会のサイバーセキュリティ・レジリエンスの強化を目指す。

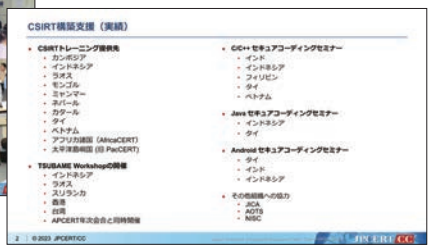
本案件を通じて、SDGs(持続可能な開発目標)ゴール9(産業と技術革新の基盤をつくろう)、17(パートナーシップで目標を達成しよう)への貢献に取り組む。

(注)CSIRT:Computer Security Incident Response Team の略。情報セキュリティ上の問題や事故が発生した場合に、適切な対応を実施する組織のことを指す。

JPCERT/CCの取組

CSIRT構築支援

JPCERT/CCは、CSIRTの基本的および国際的運営、インシデントレスポンスなど国内のCSIRTを対象としたトレーニングを提供。これにはネットワーク・トラフィック解析やマルウェア解析の実習も含まれる。ここ数年はアジア諸国(ベトナム、インドネシア、ラオスなど)やアフリカのCSIRTコミュニティでもこのような訓練を実施。



ASEAN事務局よりメッセージ

サイバーセキュリティに関する問題は、デジタル接続の増加や、クラウドコンピューティング、ブロックチェーン、人工知能などの新技術の採用が拡大することで、ますます広範かつ高度になっています。

ASEAN加盟国は地域デジタル経済の確立を目指しています。平和で安全かつ強靭な地域のサイバースペースの構築というビジョンを実現するために総力を上げなければなりません。それは経済的な発展とすべての人の生活水準の向上を可能にします。

日本とASEANの協力は、地域全体で能力と信頼を高め、サイバー脅威への対応を強化するために重要な役割を果たしています。

〈政策リファレンス〉
ASEANサイバーセキュリティ便覧を作成。
日本とASEANのサイバーセキュリティ政策の主要項目について政策リファレンスを作成・アップデート。

ASEAN事務局
デジタル・エコノミー部門
シニア・オフィサー
Arthur Glenn Maail

ASEAN各国の取組

ブルネイ Brunei Darussalam

サイバーセキュリティの課題と将来のニーズ

- サイバーセキュリティの急速な変化と、絶えず進化し高度化、組織化するサイバー犯罪の脅威
- 国境を越えたサイバーセキュリティの問題
- 国民のサイバーセキュリティに対する意識の欠如
- サイバーセキュリティの専門家と専門知識の不足

サイバーバトル キャプチャー・ザ・フラッグ 2022年大会

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	CIIの保護のためのサイバーセキュリティ令（CSO）の起草（2020）	新しいCSOの公式な発表と実施
技　術	政府向けサイバーセキュリティ インシデント報告の手続き（2021）	政府向けのサイバー演習の実施
組　織 （戦略を含む）	CSB コアサービスの ISO 27001 ISMS認証（2023年） ISO 17025 デジタルフォレンジックラボの認定（2022） 2023～2027年に向けた国家サイバーセキュリティ戦略の策定（2020年策定開始） ブルネイ国家サイバーセキュリティフレームワーク（BNCSF）（2017.10） サイバーセキュリティ協会の設立（2022.11）	ISO 27001 および ISO 17025 認証維持 国家サイバーセキュリティ戦略における国家行動計画の実行 サイバーセキュリティ令に沿ったBNCSFの見直し 協会登録・運営
能力開発	CII所有者向け重要情報インフラワークショップ（2022.10）	ー
協　力 （組織間）	CSBとブルネイ・ダルサラーム中央銀行間のサイバーセキュリティに関するMOU（2021.12） 共同サイバーセキュリティ意識向上のための CSBと通信事業者（UNN）間の契約書（LOE）（2022.11）	サイバーセキュリティ分野におけるブルネイ工科大学とのMOU サイバーセキュリティ分野におけるブルネイ・ダルサラーム大学との MOU

カンボジア Cambodia

サイバーセキュリティの課題と将来のニーズ

〈課題〉

- 適切な拘束力のある法律、戦略、基準とガイドラインの欠如
- 技術的ソリューションと産業界の参加が足りないこと
- テクノロジーソリューションの不足
- 巧妙な攻撃に対する知識とスキル
- 未だ限定的な関係機関の連携

〈協力の必要性〉

- サイバーセキュリティ戦略、標準、ガイドラインの考案
- サイバーセキュリティ人材プログラムの開発
- 能力開発と意識向上
- 情報とベストプラクティスの共有

サイバー・アンコール TTX2018

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	サイバーセキュリティ法（ゼロドラフト） フィンテック政策（ドラフト） 個人情報保護法（ゼロドラフト） サイバー犯罪法（ドラフト）	草案の改正と採択
技　術	セキュリティオペレーションセンターチーム カンボジアコンピュータ緊急対応チーム	能力向上と改善
組　織 （戦略を含む）	カンボジアのデジタル経済および社会政策枠組み 2021-2035（2021.05） カンボジアのデジタル政府政策 2022-2035（2022.01）	デジタルセキュリティ委員会の設置
能力開発	政府職員向けのデジタル スキル必須トレーニング プログラム 国民全体のサイバーセキュリティ意識 サイバーセキュリティコンテスト	サイバーセキュリティ人材の育成 サイバーセキュリティコンピテンシーフレームワーク
協　力 （組織間）	経済社会開発計画（日本政府補助金） サイバーレジリエンス向上プロジェクト（JICA事業 2023年～2026年の3年間） ASEAN（ANSAC、ASEAN-CERT、ASEAN CYBER-CC、ARF）	SOCの運用・対応能力の向上 CSIRT開発プログラム ASEAN-CERTの設立

インドネシア Indonesia

サイバーセキュリティの課題と将来のニーズ

〈課題〉

- サイバーインシデント対応、技術的リスク評価、サイバーセキュリティ戦略および政策策定などサイバーセキュリティのための有能な人材
- サイバーセキュリティと暗号技術に関する政策的な枠組みと国内規制の欠如
- AI、先端技術、オンライン詐欺など、地域における新たなサイバー脅威の発生

〈今後のニーズ〉

- サイバーセキュリティ政策が確立している他の国との二国間協力
- 国際会議、地域会議、多国間会議を通じた情報と経験の共有
- 先進的な演習や能力開発活動を提供するための他国からの援助

第14回ANSAC 2023、バリ

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	CII保護に関する大統領規則第82, 2022年	CII保護に基づく技術規制、CIIの特定、CSMの測定、サイバーインシデントへの対応、サイバーセキュリティと暗号技術に関わる人材の育成
技　術	国家安全保障オペレーションセンター（2019 - 現在） Nat-CSIRT、Gov-CSIRT、Org-CSIRT	インドネシアに121セクターのCSIRTを設立 IKNスマートシティプロジェクトの設立
組　織 （戦略を含む）	2023年大統領規則第47号 サイバーセキュリティ戦略とサイバー危機管理	国家サイバーセキュリティ行動計画（PoA） サイバー危機管理に関する内部規定
能力開発	二国間および地域のさまざまなプログラムによる能力開発に積極的に参加。（AJCCBC, ASCCE, JICA-UI, JICA 奨学金プログラム , ISPセクターのためのサイバーセキュリティ能力構築 , ASEANサイバーシールド（ACS）など。）	ー
協　力 （組織間）	IDSIRTII/CC・JPCERT 間の MOU ASEAN（ANSAC, ASEAN-CERT, ASEAN CYBER-CC, ARF, ADGSOM）	IDSIRTII/CC・JPCERT間MOU更新

ラオス Lao P.D.R.

サイバーセキュリティの課題と将来のニーズ

〈サイバーセキュリティの課題〉

- サイバーセキュリティに精通した人材の育成
- CII 部門向けのサイバーセキュリティ ポリシーの定義および策定
- 公共および民間のネットワークのサーバー／監視のためのサイバー・セキュリティ・オペレーション・センターの設立
- サイバーセキュリティツールの不足とサイバー犯罪者の追跡が困難であること
- フェイクニュースや偽情報、サービスプロバイダーやソーシャルメディアプラットフォーム会社、チャットプラットフォーム会社との情報共有

〈今後の協力ニーズ〉

- 能力開発における二国間協力
- サイバー攻撃を監視するオープンソースソフトウェアの開発支援
- 立法や戦略、政策策定などのためのサイバーセキュリティの専門知識

LaoCERT
Lao Computer Emergency Response Team

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	サイバー犯罪の防止及び対処に関する法律（2015） データ保護法（2017）	サイバーセキュリティ法の起草
技　術	サイバーセキュリティオペレーションセンター（CSOC）設立の可能性を探る。 JICA、日本の経済産業省の能力開発プロジェクトに参加	技術、ツールなどの日本への支援要請
組　織 （戦略を含む）	2012年に LaoCERTを設立 2022年に技術通信省サイバーセキュリティ局を設立	国家サイバーセキュリティ戦略の草案
能力開発	サイバーセキュリティ能力の構築：インシデント処理、インシデント対応、コンピュータフォレンジック、ネットワークフォレンジック、サイバー演習などの技術的スキル	先端技術開発のため日本への支援要請
協　力 （組織間）	JPCERT/CCとのMoM JPCERT/CCとの情報共有 NISC、ASEAN- 日本とともにサイバーセキュリティ活動を実施	サイバーセキュリティへの意識向上

ASEAN各国の取組

マレーシア Malaysia

サイバーセキュリティの課題と将来のニーズ

〈課題〉

- サイバーセキュリティガバナンス
- 人事および技術専門家
- 限られた法的枠組み
- 国民の認識不足
- サイバー脅威の急速な進化
- 限られた財源

〈今後のニーズ〉

- さらなる技術トレーニングと能力開発
- 産業用制御システム（ICS）や新技術などのニッチな分野でトレーナー研修の提供
- 将来のサイバー人材を育成するための大学との協力
- 専門家と技術能力に関する産業界とのパートナーシップ
- サイバーエコシステムを促進するためサイバーセキュリティ関係者との協力

CYDES オープニングスピーチ

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	国家サイバーセキュリティ政策（2010） ISO/IEC 27001：重要な国家情報インフラ（CNII）機関に対する情報セキュリティ管理システム標準の導入の閣議決定（2010年2月24日） 2010年個人データ保護法 国家サイバー危機管理計画（NCCMP）（2011） 国家安全保障会議指令 No. 24: 国家サイバー危機管理の政策と仕組み（2011） 国家暗号化政策（2013） 国家安全保障会議指令 No.26: 国家サイバーセキュリティ管理（2021）	マレーシアサイバーセキュリティ法案 サイバーセキュリティに関する新しいガイドラインと回覧
技　術	マレーシア国家サイバー調整指揮センター（NC4）の設立 公共部門のサイバー セキュリティ フレームワーク 2016 CNII 機関に対する技術勧告の発行 技術規定 - 情報とネットワークのセキュリティに関する要件 クラウドコンピューティングガイドラインにおける公共部門の情報セキュリティ管理 公共部門のサイバーセキュリティインシデント管理に関する回覧 2022年 国家コンピュータ緊急対応チーム（CERT）の設立	マレーシア国家サイバー調整指揮センター（NC4）の強化
組　織 （戦略を含む）	2017年国家サイバーセキュリティ局（NACSA）の設立 2010年国家サイバー セキュリティ政策 2020-2024年マレーシアのサイバーセキュリティ戦略 国家サイバーセキュリティ意識向上基本計画の策定	サイバーセキュリティにおけるマレーシアのガバナンス構造の効率化 サイバーセキュリティのための専用運営支出
能力開発	全国サイバー訓練演習（X-Maya）　CYDES2020 部門別サイバー訓練　ICTSO 2022 ネットワークセキュリティに関する産業講演 ISMS・BCMS認定研修（毎年）	CYDES 2023 ICTSO 2023
協　力 （組織間）	2021-2025年 ASEANサイバーセキュリティ協力戦略 サイバースペースにおける国家の責任ある行動に関するUNGGE規範実施のASEAN地域行動計画（RAP）マトリックス マレーシア・日本サイバーセキュリティ政策対話	ー

ミャンマー Myanmar

サイバーセキュリティの課題と将来のニーズ

- 人材の不足
- 法的要件による規制や政策の実施の制限
- サイバーセキュリティに関する正式な法律がないため、サイバーセキュリティ産業とサイバー関連の問題の調整に規制上の制限が生じること
- CSIRT、ISAC、セキュリティ監査などのサイバーセキュリティ機関の専門的な権限を持つ組織構造の問題
- 新型コロナウイルス感染症のパンデミック前と同様のJICAによる能力開発研修プログラムの実施
- 政策レベルと運用レベルの両方に対する能力開発のサポート
- さらなる技術面での協力

ミャンマーのサイバーセキュリティへの挑戦（2023年）

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	コンピュータサイエンス開発法（1996年） 電子取引法（2004年）、改正（2014年、2021年） 電気通信法（2013年）改正（2017年） サイバーセキュリティ政策が、2022年12月に開催されたミャンマー連邦政府会議（No.9/2022）により承認	サイバーセキュリティ法
技　術	ミャンマーコンピュータ緊急対応チーム（mmCERT/cc） セキュリティ オペレーション センター（GSOC）	政府機関における分野別CSIRTの設立を奨励 24時間365日の政府機関向けオンデマンド・プロテクション
組　織 （戦略を含む）	運輸通信省 - MoTCはミャンマーにおける情報セキュリティを含む ICT 関連政策を担当 情報技術およびサイバーセキュリティ部門（ITCSD）は、さまざまな部門の電子政府プロジェクト / プロセスの協力と調整、電子政府プロジェクトの実施、ICT 標準化、サイバーセキュリティの監督と技術的助言、およびサイバーセキュリティ法、サイバー政策とフレームワークの実施を担当 国家サイバーセキュリティセンター（NCSC）は、すべての省庁がオンラインサービスを安全に提供でき、すべての国民が電子政府サービスに安全にアクセスできる環境の構築するとともに、サイバーセキュリティ意識向上プログラムを国全体に展開する役割を担当	サイバーセキュリティポリシーに基づく組織体制の拡充
能力開発	日本とミャンマーが共同開発した啓発冊子「サイバーセキュリティを学ぼう」を発行。2022年に再版され、ネピドーの MICC-2で開催された「青少年、文学、アートのショー」で配布 2021年に電子ブックレット「モバイルデバイスのサイバーセキュリティ」の共同意識向上活動に貢献。「モバイルデバイスのランサムウェア」というテーマで参加。2022年にA5サイズの小冊子として再版され、政府機関に配布 ASEAN- 日本サイバーセキュリティ啓発ビデオ・コンペティションへの参加者を選ぶため、「ミャンマー・サイバーセキュリティ啓発ビデオ・コンペティション -2023」を開催 JPCERT/cc と mmCERT/cc は、2011年、2012年、2013年、2015年に、ネットワーク・フォレンジック、マルウェア分析、高度なマルウェア分析、インシデント処理、および高度なインシデントハンドリングのコースを共同で開催しました。この期間を通じて、政府機関や民間金融部門からの参加者は250名超 ITCSDの従業員を 2019年から AJCCBC サイバーセキュリティ技術トレーニングコースをオンサイトとオンラインの両方の受講のために派遣 2019年、2020年、2021年に日本でオンサイトおよびバーチャルで開催された「サイバー攻撃に対する防御演習」研修コースに参加者を派遣 AJCCBCの支援を受け、2020年と2021年に政府機関職員向けに「自己学習トレーニングコース ローカライズ版」を提供 2019年と 2022年にASEANサイバーSEAゲームの参加者選考のため、ミャンマーサイバーセキュリティチャレンジを開催	啓発冊子とポスターが作成され、地域の展示会、ワークショップ、意識向上プログラムで配布 「日本・ASEAN サイバーセキュリティ啓発ビデオコンペティション 2023」に参加 今年度、サイバーセキュリティ啓発ショートムービーを放送・掲載する予定 国際プログラムを通じて得た知識を応用し、現地研修、知識共有セッション、意識向上プログラムが実施 大学や高校での意識向上プログラムやイベントを推進 要望に応じて大学生にインターンシップ・プログラムを提供 ミャンマー・サイバーセキュリティ・チャレンジを毎年開催し、サイバーセキュリティのスキルを向上させ、サイバーセキュリティの専門家の能力を高める
協　力 （組織間）	APCERTの運営メンバーとして会議、セミナー、訓練に参加 ASEANネットワークセキュリティ評議会（ANSAC）に参加 ASEANサイバーセキュリティ調整委員会（ASEAN Cyber-CC）に貢献 ASEAN - 日本サイバーセキュリティ政策会議やワーキンググループ会議に参加 ASEAN・日本遠隔サイバー演習、ACID訓練、ITU訓練、ASEANサイバーSEAGames を毎年実施 2019年に日本の総務省とミャンマーの運輸・通信省と共同で「ミャンマーサイバーセキュリティワークショップ」を開催 2019年にCLMV諸国のための国際サイバーセキュリティ政策と外交に関する第4回上級レベルワークショップを主催 2017年の第3回ASEAN・日本WG会議、2022年の第3回ASEANサイバーCC会議で共同議長を務めた 2022年に第13回ANSAC会議をバーチャルで開催	サイバーセキュリティ関連の組織間の関係強化のため、国際協力、地域協力、地方協力への貢献を継続

フィリピン Philippines

サイバーセキュリティの課題と将来のニーズ

・国内にはサイバーセキュリティの専門家が不足している。2016年には、インドネシアの107人、タイの189人、マレーシアの275人に対し、フィリピンには CISSP認定専門家が84人しかいなかったと報告されている。そして、84人全員がフィリピンに拠点を置いているわけではなく、彼らのほとんどは海外で働いていた。現在、(ISC)2ウェブサイトによると、国内にはすでに216のCISSPが存在しますが、業界が必要とする専門家の数を満たすにはまだ少なすぎる。パートナーシップによってサイバーセキュリティのための教育プログラムを発展させることができるかもしれない

・CERTの能力開発。CIIごとに部門別CERTリーダーが特定されているが、主な課題は CERT を担当できる人材の不足とセキュリティ オペレーション センターがないこと

・サイバーセキュリティ基準の必要性。最新のグローバル サイバーセキュリティ指数(GCI)でフィリピンのスコアが低かった領域の 1つは、サイバーセキュリティ標準の国家的枠組みの採用。DICTは昨年以降、ICT機器や重要資産のリスクを軽減することでサイバー攻撃を軽減または防止するサイバーセキュリティ基準の導入に取り組んでいる

国家サイバーセキュリティ計画2028関係者協議
(ビサヤ支部)

取組と今後の計画

カテゴリー	実施内容	今後の計画
法 定	2012年サイバー犯罪防止法および2012年データプライバシー法の制定 情報通信技術省を創設する2015年DICT法の制定	サイバーセキュリティ法　CII 保護法(上院法案) CIIに対する最低限の情報セキュリティ基準を義務付ける大統領令
技 術	2018年に国家コンピューター緊急対応チーム(CERT-PH)を創設 2018年に国家サイバーセキュリティ オペレーション センター(NSOC)を発足 毎年恒例のサイバー訓練　政府機関向けの脆弱性評価と侵入テスト サイバーセキュリティ評価プロバイダーの認定	—
組 織 (戦略を含む)	2022年国家サイバーセキュリティ計画の策定 国家安全保障戦略12項目にサイバーセキュリティを含める 2028年フィリピン開発計画(PDP)にサイバーセキュリティを盛り込む	国家サイバーセキュリティ計画 2028策定(2023年5月30日に発表予定)
能力開発	JICA技術能力向上プロジェクト　サイバーセキュリティの擁護活動と啓発キャンペーン サイバーレンジプラットフォーム	—
協 力 (組織間)	国家サイバーセキュリティ省庁間委員会(NCIAC)の創設 サイバー脅威の監視と情報共有　国家サイバーセキュリティ機関間委員会(NCIAC)	—

シンガポール Singapore

サイバーセキュリティの課題と将来のニーズ

〈課題〉

オペレーショナル・テクノロジー(OT)システムを標的とするサイバー脅威の能力と影響力の増大
・OTシステムは通常、必要不可欠なサービスを支えているため、侵害されると深刻な結果を招く可能性がある

ランサムウェアの脅威のほぼすべての業種・業界への拡大
・ランサムウェアグループが大規模な基幹サービス・プロバイダーを標的にする傾向があることが懸念される

地政学的な緊張と紛争における非国家主体の役割
・多くの非国家主体には、紛争の方向性や規模を決定する大きな力と影響力がある

〈今後のリスク〉

・**風評被害のためのランサムウェア(R4R)** - ランサムウェアグループは、暗号化よりもデータ流出に注目するようになり、企業に風評被害を避けるための支払いを要求する犯罪がますます増えている

・**諸刃の剣となる人工知能(AI)** - AIはサイバー犯罪者の能力を増幅させる可能性がある

・**量子コンピューティングとデジタル・セキュリティ** - 犯罪者は量子コンピューティングを悪用し、ウェブサイトやモバイルアプリケーションを保護する暗号化アルゴリズムを侵害する可能性がある

第7回サイバーセキュリティに関するASEAN閣僚会議

取組と今後の計画

カテゴリー	実施内容	今後の計画
法 定	サイバーセキュリティ法(2018)　コンピュータ不正利用防止法(1992) 重要情報インフラ(CII)のためのサイバーセキュリティ実施規範 2.0(2022年)　個人情報保護法(2012)	サイバーセキュリティ法2018の継続的な見直し
技 術	シンガポールコンピュータ緊急対応チーム(CERT) ASEAN CERT インシデント訓練(ACID) SingCERT による ASEAN 情報共有セッション CII のためのセキュリティ・バイ・デザインの枠組み CII のためのサイバーセキュリティ・リスク評価の実施ガイド CII 所有者のための 5G ユースケース強化ガイドライン CII のためのサイバーセキュリティ監査ガイドライン CII のためのサイバー脅威モデリングガイド CII サプライチェーン・プログラム・ペーパー 運用技術のサイバーセキュリティ・コンピテンシー・フレームワーク IoT と医療機器のサイバーセキュリティ・ラベリング制度 シンガポール標準規格計画 サイバーセキュリティサービスプロバイダーのためのライセンスフレームワーク 最新のサイバーセキュリティのトピック、トレンド、テクノロジーに関する月刊サイバーセンス・ニュースレターの発刊 サイバーセキュリティ認証制度 サイバー・エッセンシャル・マーク サイバー・トラスト・マーク 組織向けサイバーセキュリティ・ツールキット 組織のためのサイバーセキュリティ・ヘルスプラン	—
組 織 (戦略を含む)	シンガポール・サイバーセキュリティ戦略(2021-2025年) シンガポール運用技術サイバーセキュリティ基本計画 シンガポール・サイバースペース基本計画 シンガポールの年間のサイバーセキュリティ状況の報告書(2016-2022年)	—
能力開発	ASEAN- シンガポール・サイバーセキュリティ・オブ・エクセレンス 国連シンガポールサイバーフェローシップを含む、ASEAN加盟国とその他の国際パートナーのための能力開発プログラム CSA アカデミー 国家および部門レベルのサイバー演習 国民の意識啓発(GoSafeOnline のウェブサイト) SG サイバー人材育成基金 SG サイバーシリーズ(タレント、ユース、オリンピック出場者、教育者、女性、指導者)	—
協 力 (組織間)	シンガポール国際サイバーウィーク OT サイバーセキュリティの専門家パネル サイバーセキュリティ業界のイノベーションの呼びかけ ブロック 71 におけるイノベーション・サイバーセキュリティ・エコシステム 国家サイバーセキュリティ研究開発プログラム CSA とナンヤン工科大学による国立評価統合センター CSA は 11 の重要セクターのリーダーとの協力により、CII サイバーインシデントの保護、対応、調査を実施	—

ASEAN各国の取組

タイ Thailand

サイバーセキュリティの課題と将来のニーズ

〈課題〉
- 人、政策、知識、システムなど、すべての構成要素のエコシステムとサイバー・キャパシティを構築する。
- 強力なパートナーシップと統合された取り組みによる相乗効果の構築
- CIIと政府サービスの回復力の向上
- 世界トップクラスのサイバーセキュリティ組織となるよう努力する

〈協力の必要性〉
- 国間の信頼構築と情報共有
- 国際卓上演習
- サイバー脅威に対処するための国際協力
- サイバーオペレーションに関する国際法の訓練とワークショップ
- OTシステムの一部におけるサイバーセキュリティ教育のための産業界との協力

AJCCBC 開所式2018

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	コンピュータ犯罪法 2007年、2017年 2019年個人データ保護法 サイバーセキュリティ法 2019（国家サイバーセキュリティ庁：NCSA）	サイバーセキュリティの標準と成熟度を高めるための二次的な法律、規制、ガイドラインを実施し、施行 重要情報インフラ組織に対する最低限のセキュリティ基準の提供
技　術	タイコンピュータ緊急対応チーム（ThaiCERT） セクター CERTの設立	将来の脅威に備えるためThaiCERTのサイバーセキュリティ能力を強化 脅威情報の共有の促進と支援
組　織 （戦略を含む）	この法律で規定された重要情報インフラ（CII）組織は、セキュリティ要件の標準的枠組みに準拠しなければならない NCSA は、CIIの組織のためのガイドラインとして、サイバーセキュリティの実践規範と標準的な枠組みを策定する サイバーセキュリティ政策と行動計画（2022年～ 2027年）に関する国家サイバーセキュリティ委員会の発表 " 経済と社会の持続可能性を確保するためのタイの重要なサービスのためのサイバーセキュリティ " 長期的な成功と進歩のためにサイバーセキュリティ政策と行動計画を推進する 政府サービスと重要な情報インフラに対するサイバー・レジリエンスの推進	重要情報インフラ組織に対する最低限のセキュリティ基準の提供 重要情報インフラ組織のための規制構造と法的枠組みの確立 政府機関のデータシステムとネットワークの保護
能力開発	労働力、知識、技術を統合することにより、国のサイバーセキュリティ能力を構築し、サイバーセキュリティ・イノベーションを発展させる さまざまなプログラムを通じたサイバーセキュリティ人材の能力開発 NCSAは、2022年に400名の専門家と幹部を含む2,250名の参加者を対象とした集中的な能力開発プログラムを通じて、CIIの組織が国際基準を満たすためのサイバーセキュリティ能力を開発 NCSAとJICAは、AJCCBCが運営する「サイバーセキュリティと信頼されるデジタルサービスのための日ASEAN能力構築プログラム強化プロジェクト」に関する協議記録に署名した	サイバーセキュリティ人材の増加 サイバーセキュリティに対する意識とスキルの向上 イノベーションを含むサイバーセキュリティの研究開発の促進
協　力 （組織間）	国内および国際機関の協力と連携を求める サイバー脅威への対応と重要なサービスの通常業務への復旧に備え、国内外の協力を統合する。 NCSAは、CIIの７部門（国家安全保障、公共サービス、銀行・金融、情報技術・通信、輸送・物流、エネルギー・公共事業、公衆衛生）に対して、サイバー脅威によるリスクを防止・軽減するための支援を提供する役割を担っている	官民連携の推進と支援 サイバー脅威に対処するための国際協力の調整

ベトナム Viet Nam

サイバーセキュリティの課題と将来のニーズ

〈課題〉
- サイバーセキュリティの急速な変化と、絶えず進化し高度化、組織化するサイバー犯罪の脅威

〈協力への課題〉
- 基準とガイドラインの策定
- サイバーセキュリティ人材育成プログラム
- 能力開発と意識改革
- 情報とベストプラクティスの共有

通信情報省事務局

取組と今後の計画

カテゴリー	実施内容	今後の計画
法　定	2015年サイバー情報セキュリティ法 2018年サイバーセキュリティ法	新たなサイバーセキュリティの課題に取り組むための政策、規制の提案
技　術	ベトナムサイバーセキュリティ緊急対応チーム / コーディネーションセンター VNCERT/CC 国家サイバーセキュリティセンターNCSC	SOCオペレーションと対応能力の改善 CSIRT開発プログラム
組　織 （戦略を含む）	情報セキュリティ当局（AIS）がベトナムのサイバーセキュリティ分野の国家行政を担当	ベトナムサイバーセキュリティ戦略の実施 国家デジタルトランスフォーメーション実施の促進
能力開発	サイバーセキュリティに関する新たな政策や規制、方策の提案 サイバーセキュリティ人材の育成における2025年基本計画（サイバーセキュリティ意識向上とサイバー・レジリエンス）	基本計画の実施と１年ごとの結果の検証
協　力 （組織間）	ASEAN（ANSAC, ASEAN-CERT, ASEAN CYBER-CC, ARF） ASEAN +（ASEAN- 日本 , 米国）, ITU APCERT, FIRTST, CAMP	SOCオペレーションと対応能力の改善 CSIRT開発プログラム

日本の主な取組例

総務省の取組

ASEANにおけるサイバーセキュリティの能力構築への協力

バンコク（タイ王国）において、「日ASEANサイバーセキュリティ能力構築センター」が設立され、平成30年9月14日に同センターの開所式が開催されました。総務省としては、この取組を契機に、ASEANにおけるサイバーセキュリティの能力構築への協力を更に強化に取り組む。

①これまでの活動とその成果

2009年から現在までに、ASEAN地域で実施したサイバーセキュリティ関係事業について

＜AJCCBC＞

活動年度 ▶ 2018-2022

活動内容 ▶ AJCCBCの円滑な運用

成　　果 ▶ 1,000人を超える受講生の輩出

功労者（表彰者）の候補 ▶
＜AJCCBC＞ETDAチャイチャナ長官以下関係者

②今後の予定、検討中の事業

今後の予定、期待する事項（ASEANに関係する問題意識等）

＜AJCCBC活動の拡大＞

既存の活動の参加者拡大 ▶
各国政府関係者および、CIIのICTスタッフの参加促進

将来的なAJCCBCの活動範囲の拡大 ▶
演習対象やコンテンツの拡充を推進

※JASPER：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」の共同声明で合意されたネットワークセキュリティ分野における技術協力を強化するための日ASEAN技術協力プロジェクト。インドネシア、シンガポール、タイ、フィリピン、マレーシア、ミャンマー、ラオスが参加（ミャンマー、ラオスはDAEDALUSのみ）

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）における新プロジェクトの開始

2023年6月19日に日ASEANサイバーセキュリティ能力構築センター（ASEAN-Japan Cybersecurity Capacity Building Centre：AJCCBC）において、国際協力機構（JICA）の技術協力プロジェクト「サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト」の開始にかかるセレモニーが開催。
AJCCBCへの演習の提供や演習プログラムの充実化を通じ、今後もASEANにおけるサイバーセキュリティの能力構築への協力を継続。

経済産業省の取組

インド太平洋地域における日米欧ICSサイバーセキュリティ週間

経済産業省とICSCoEは、米国政府（DHS/CISA、DOS）および欧州委員会（DG CONNECT）と共同で、第6回日米欧産業制御システム（ICS）サイバーセキュリティ週間を2023年10月に開催。

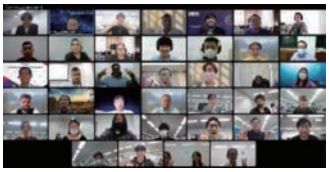
〈日付〉2023年10月9日～13日
〈概要〉日本で開催し、インド太平洋地域（ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾）から約40名のコア参加者が参加し、実践的な演習を行う。また、日米欧の専門家によるランサムウェアやサイバーインシデ ントなどの最新動向を含むサイバーセキュリティ関連セミナーを実施。

昨年の練習風景

植村 昌弘
経済産業省大臣官房審議官

エリック・ゴールドシュタイン
サイバーセキュリティ担当
エグゼクティブ・アシスタント・ディレクター、
CISA

ロレーナ・ボイックス・アロンソ
DG CONNECTディレクター



インド太平洋地域からの参加者

防衛省の取組

サイバーセキュリティ能力構築支援事業

ASEAN地域で実施したサイバーセキュリティ関係事業について

活動年度	2017年度～2022年度（2022年度で事業は終了）
活動内容	ベトナム人民軍におけるサイバーセキュリティ能力の向上に寄与するため、3回のセミナーにより基礎的知識及び技能を教育し、その後、オーストラリア軍のオブザーバー参加のもと定着度確認を実施。
成　　果	定着度確認を経て、3回のセミナーの成果が十分に発揮されたことを確認。結果、ベトナム人民軍のサイバーセキュリティ能力を向上させることができた。

活動年度	2021年度
活動内容	2022年2月、ASEAN地域の各国に対し、インシデント対応能力の向上を図ることを目的としたセミナー（インシデント発生時に対処するために必要な知見の共有や実技）をオンラインにて実施。
成　　果	参加20名がサイバーセキュリティの基礎について理解
今　　後	今後の予定は、2023年度に第2回事業を実施する予定

次の10年に向けて Looking ahead to the next decade

国際協力機構（JICA）
最高デジタル責任者
戸島 仁嗣

JICAは2022年末にサイバーセキュリティ・クラスター事業戦略 を策定しました。これは同分野での開発途上国への協力経験を踏まえたものです。
本戦略は、ITUのGlobal Cybersecurity Agenda モデルを基に、5つの能力要素における4つの発展段階を提示。JICAは、対象国の状況を見極めながら、最適な支援を推進します。ASEAN諸国とは、2023年に開始した日ASEANサイバーセキュリティ能力強化センター（AJCCBC）との協力で、今後4年間で500名以上の人材育成を行う等、事業を拡大しています。
今後も、JICAは、サイバー空間で深刻化しつつある脅威に対応し、人々の生活と尊厳を守ることのできる社会の実現（Cybersecurity for All）を目指し、日本政府やパートナーと共にASEAN諸国の更なる発展に協力していきます。

サイバーセキュリティ・クラスター事業戦略

JPCERT/CC
国際部部長
小宮山 功一朗

日ASEAN友好関係を振り返って、苦しい10年間だったと言っていいのではないでしょうか。グテーレス国連事務総長は、世界が「信頼欠乏症」に侵されていると表現しました。その言葉はサイバー空間にも当てはまります。この10年で、国家が関与する大規模なサイバー攻撃や高度なサーベイランス活動の存在が明らかになりました。国境を超えた協力は、その意義を問われることとなり、仰ぎ見れば、これからの10年の日ASEAN関係は明るいでしょう。信頼欠乏症に苦しむ国際社会において、日ASEANは変わらず友情と信頼を育んできました。私自身も、すべてのASEAN加盟国に虚心坦懐に話すことのできる友人がいます。組織によらず、政治的な状況によらず、何でも相談できる。本会議にご参加いただいた古くからの友人と、そしてまだ見ぬ新しい友人と、共に日ASEAN間の協力を模索していきたいと思います。

JNSA会長
東京大学大学院
情報理工学系研究科 教授
江崎 浩

インターネットは、多様な組織が構築・運用するデジタル資源を相互接続し、地球上にシェアリングエコノミー型デジタルインフラストラクチャーを構築しました。その結果、地球上のすべての人とデジタル機器（Things）が国境を越えてネットに接続され、自由なデータ交換を可能にする進化を遂げました。我々は、これまでインターネットへの接続を想定する必要がなかった人やデジタル機器が接続されることを前提にしたサイバーセキュリティーを実現しなければならなくなったのです。これまで以上に関係者の力を持ち寄り、新しい仲間と力を合わせ、共によりよいグローバルなデジタル空間を作り出し、それを次世代に引き継ぐ責任を果たさなければなりません。