

国際連携に関する最近の取組

令和5年2月1日

サイバーセキュリティタスクフォース事務局



2023年1月 EU: NIS (Network and Information Security) 2指令
NIS指令を改正し、関係セクターの監督権の強化、加盟国CSIRT間の連携強化、ENISAによるEU全般への情報提供・連携における権限強化を実現する指令で理事会で2022年12月に承認され、翌年1月に施行された。今後EU加盟国は21ヶ月以内に国内法を整備する必要がある。

2022年9月 EU: サイバーレジリエンス法案

EU域内市場に上市されるあらゆるデジタル製品(ソフトウェアを含む)に関して、一定のサイバーセキュリティ要件の遵守や、製造業者による最低5年間のセキュリティアップデートの提供や脆弱性及びインシデントの当局への報告を義務づけるもの。欧州委員会で提案され、欧州理事会及び欧州議会にて議論予定。



2022年10月 「電気通信(セキュリティ対策)規則」施行

2021年の電気通信法の改正にもない、「電気通信(セキュリティ対策)規則」が施行。公共ネットワークプロバイダにセキュリティ対策を確実に実行するように求める。Ofcom(通信庁)が規則の施行を実施し監督する。規則に違反した場合は最高で売り上げ10%の罰金、継続的な場合は10万ポンドの罰金が科される。本規則を遵守するための技術的なガイダンスであるCode of Practiceが同年12月に公表されている。



2023年1月 NTTがJCDCに参加

NTTがサイバーセキュリティとレジリエンスに対する米国政府の国際的取り組みをさらに強化するためのイニシアティブである共同サイバー防衛連携(Joint Cyber Defense Collaborative(JCDC))のメンバーに加入。



2022年5月 米豪印戦略対話(QUAD)

首脳会談で「日米豪印サイバーセキュリティ・パートナーシップ」共同原則が公表された。



2022年7月 重要インフラ法・電気通信法改正

サイバーインシデント発生時の報告義務を定めた法律が施行。サービス停止等の重大な影響を及ぼすインシデントについては12時間以内、個人情報流出等の被害については72時間以内の報告を義務づけ。

- サイバー空間は国境を越えて利用される領域であることから、**各国政府・民間レベルでの情報共有や国際標準化活動**に積極的に関与。
- また、世界全体のサイバーセキュリティのリスク低減のため開発途上国に対する**能力構築支援**を行うほか、国内企業の**国際競争力向上**を図る取組も推進。

● 有志国との二国間連携の強化

サイバー協議等の場を活用した情報発信、意見交換等の実施。

● ISACを通じた民間分野での国際連携の促進

海外ISACとの連携推進、ASEANとのISPワークショップ等の実施。

● 国際標準化機関における日本の取組の発信及び各国からの提案への対処

国際電気通信連合関係会合
(ITU-T SG17) への参加。

● 多国間会合を通じた有志国との連携の強化

日米豪印 (Quad)、OECD、日ASEANサイバーセキュリティ政策会議等の多国間の枠組みを活用した情報発信、意見交換等の実施。

● インド太平洋地域における開発途上国に対する能力構築支援

日ASEANサイバーセキュリティ能力構築センター (AJCCBC)
による支援

- ✓ サイバーセキュリティ演習の実施
- ✓ Cyber SEA Game開催（若手技術者・学生参加の競技会）
(2018-22年で948人参加)

● 国際展開支援

サイバーディフェンスセンター (CDC) の普及展開活動、日本企業のサイバーセキュリティソリューション・製品等の国際展開を目的とした実証事業等の実施。

- 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（電子取引開発機構）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

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



日ASEAN情報通信大臣会合
（2017年12月）

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。
- 2023年1月時点で計 **1,148名** が参加。（目標である4年間で700人程度の育成を達成）



サイバーセキュリティ演習模様

運営体制の強化

- AJCCBCの運営については、これまでJAIF（日・ASEAN統合基金）を活用してきたが、来年度からJICAの技術協力プロジェクトとして位置付けられる予定。
- AJCCBCの事務局機能については、これまでタイ政府のETDA（電子取引開発機構）が担ってきたが、今年春以降にNCSA（国家サイバーセキュリティ庁）に移管される予定。

第三国との連携による演習プログラムの充実化

- 昨年はスイス及び英国からコンテンツや講師等の提供を受けて演習を実施。
- 新たに米国からコンテンツ等の提供を受けて本年夏頃に演習を実施予定。

演習対象の拡大

- AJCCBCの更なる活性化やASEAN域内への貢献に向けて、演習を提供する対象を学術機関へ拡大することを検討中。
- 来年度にASEAN域内及び日本の学術機関と連携し、大学生や初・中等教育向けのサイバーセキュリティ教育をテーマとしたワークショップを開催予定。

他地域への展開

- AJCCBCで得られた知見・ノウハウを活かし、新たに大洋州島しょ国を対象としてサイバーセキュリティ能力構築支援プロジェクトを立ち上げることを検討中。米国や豪州等とも連携していく予定。
- 今年度は対象国におけるニーズ等を把握するための調査を実施中であり、調査結果を踏まえ、来年度中を目途にプロジェクトの立ち上げを目指す。

首脳会合共同声明（サイバー関係抜粋・仮訳）

高度化するサイバー脅威を伴うデジタル世界が拡大するなかで、我々は、サイバーセキュリティを強化する集団的アプローチを取るこ
とが緊急に必要であることを認識した。

我々は、自由で開かれた、包摂的なインド太平洋に関する日米豪印首脳のビジョンを実現するため、脅威情報の共有、デジタル対応製品及びサービスのサプライチェーンにおける潜在的なリスクの特定・評価、及び全ての利用者が利益を享受できるよう、より広範なソフトウェア開発のシステムを改善するため、政府調達のための基本的なソフトウェアセキュリティ基準の整合並びに我々の集団的な購買力の活用によって、我々の国の重要インフラ防護を改善することにコミットする。

「クアッド」のパートナーは、「クアッド・サイバーセキュリティ・パートナーシップ」の下でインド太平洋地域の能力構築支援プログラムを協調するとともに、「クアッド」各国、インド太平洋地域及びそれ以外の地域における個々のインターネット・ユーザーが、サイバー脅威から自らを守ることを支援するべく、史上初の「クアッド・サイバーセキュリティ・デイ」を開始する。

【共同原則（Joint Principles）】

- ・ 2021年9月の会合立ち上げ後、「重要インフラ保護」、「サプライチェーンリスク管理」、「ソフトウェアセキュリティ」、「人材育成」の4つをテーマに行われた議論の成果を取りまとめたもの。

①重要インフラ保護

重要インフラ保護に資する脅威情報その他のセキュリティ情報の共有（4極の政府・民間間）を促進。

②ソフトウェア等のセキュリティ確保

ソフトウェアのセキュリティに関する最低限の基準（脆弱性情報の管理、SBOM、多要素認証、セキュリティ管理システムの監査等）の策定に向けた協働を推進。特に、ソフトウェアの政府調達におけるセキュリティ確保の枠組みの確立に向けた協働を実施。

③サプライチェーンのレジリエンス・セキュリティの確保

サプライチェーンにおける潜在的脅威の特定やサプライチェーンリスクへの依存度を評価するための枠組みの確立に向けた協働を実施。また、関係する基準やガイドライン等に関する意見交換を実施。

④人材育成

インド太平洋地域における能力構築支援プログラムに係る協働・連携を実施（Quadサイバーセキュリティ・パートナーシップ）。

結果概要

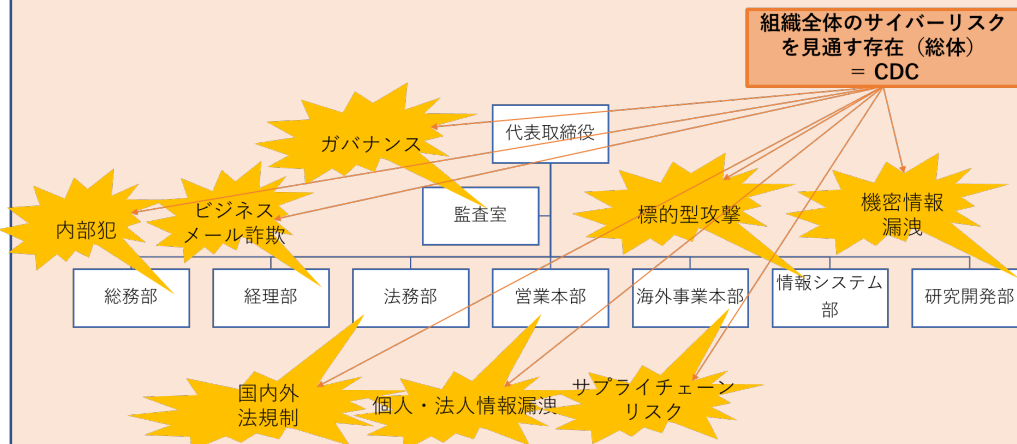
- 「5Gセキュリティガイドライン第1版」の勧告化に向けた検討の合意
- 次期ITU-T総会（WTSA-24）に向けたコレスポンデンスグループ（CG）の設立
 - 次期（2025-2028）におけるSG17のマンデートや課題構成等について議論が行われる。CG共同議長にWP2議長の三宅優氏（KDDI総研）が就任

	課題名	
SG17	セキュリティ	
WP1	セキュリティ戦略と調整	WP4 サービスとアプリケーションのセキュリティ
Q1	セキュリティ標準化戦略と連携	Q7 安全なアプリケーションサービス
Q15	量子ベースのセキュリティを含む 新しい技術のための／によるセキュリティ	Q8 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
WP2	5G、IoT及びITSセキュリティ	Q14 分散型台帳技術（DLT）のセキュリティ
Q2	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	WP5 根源的なセキュリティ技術
Q6	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	Q10 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
Q13	高度道路交通システム（ITS）セキュリティ	Q11 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）
WP3	サイバーセキュリティとマネジメント	
Q3	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	
Q4	サイバーセキュリティと迷惑メール対策	
Q10	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	
Q11	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)	

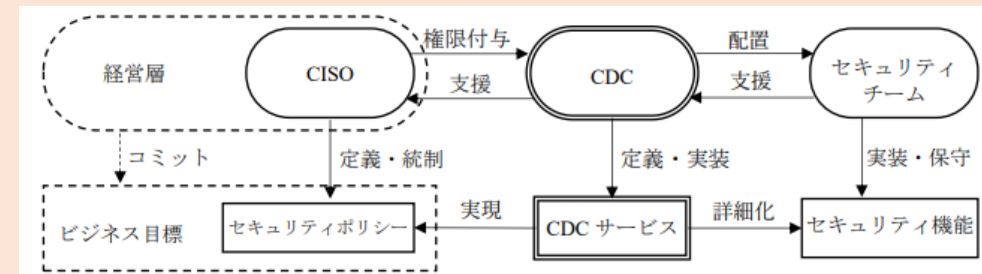
- ITUにおいて議論されていたサイバーディフェンスセンター（CDC）が、2021年10月、ITU勧告X.1060（the Framework for creation and operation of a cyber defense centre）として発行された。
- 本勧告には、日本発のサイバーセキュリティの知見として、政府や各省庁、民間セキュリティ団体の政策やノウハウが取り入れられている。
- サイバーセキュリティ体制の構築が遅れている発展途上国を対象にCDCの普及展開活動を実施することにより、サイバーセキュリティ分野における我が国の国際的なプレゼンス向上を図る。

サイバーディフェンスセンター(CDC)とは

- 組織活動がデジタル化するにつれ、情報システムへの脅威が、単にシステムへの被害を発生させるだけでなく、経営的な被害や、より物理的あるいは人的な被害までも引き起こすようになったことを受け、組織全体のサイバーセキュリティリスクを俯瞰する存在が必要。
- CDCはセキュリティポリシーに沿った組織のセキュリティを確保するため、セキュリティサービスをカタログ化・実施組織の選定及び目標スコアの設定を行い（構築：Build）、それらを短期・長期的なマネジメントによって運用（Management）、さらに定期的な評価（Evaluation）を行う。



CDCは組織が受ける恐れのあるセキュリティリスクを俯瞰し、情報システムに留まらない、より広い範囲のリスクに対抗。



CDCはCISO（最高情報セキュリティ責任者）の策定したセキュリティポリシーを実現するために、組織内のセキュリティチームや機能の最適化・指揮を行う（CDCサービスの実施）