資料３－１

国際連携に係る取組状況

令和6年3月13日

事務局

最近のサイバーセキュリティに関する諸外国の主な動向

2024年3月 「サイバー連帯法」とサイバーセキュリティ法（CSA）の改正

欧州連合理事会は、理事会議長と欧州議会の交渉担当者が、「サイバー連帯法」とサイバーセキュリティ法（CSA）の対象を絞った改正に関する暫定合意に達したと発表した。サイバー連帯法の改正は、サイバーセキュリティの脅威およびインシデントの検出・認識を支援する等を目的としており、CSAの改正は、マネージドセキュリティサービスの認証スキーム等に言及する等、レジリエンスの向上となるもの。

2024年3月 「サイバー危機管理のためのベストプラクティス」

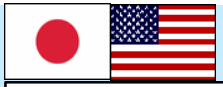
欧州連合サイバーセキュリティ機関（ENISA）は、危機管理強化を支援する「サイバー危機管理のためのベストプラクティス」を公表した。同書は、サイバー危機管理サイクルを4つのフェーズ（予防、準備、対応、復旧）に分類し、各段階で発生する問題への取組を示すもの。

2024年1月 「サイバーセキュリティ認証スキーム」

欧州委員会は、EUサイバーセキュリティ法（CSA）に沿って、初のサイバーセキュリティ認証スキームを採択したと公表した。スキームは、ハードウェアとソフトウェアを保護するため情報通信技術の製品をライフサイクルで認証するもので、NIS2指令の実施を促進する。

2023年7月 「国家安全保障法案」成立

英国の国家安全保障法案が両院を通過し、成立した。この新法は、英国のスパイ防止法を抜本的に見直し、法執行機関及び情報機関の活動をしやすくするという。加えて、英国の民主主義に不可欠な基本的権利を妨害する行為は違法となり、これらの権限は、偽情報やサイバー攻撃、選挙妨害等、あらゆる形態の悪質な活動にも適用される。



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。

2024年2月 「Cybersecurity Framework（CSF）」の第2.0版を公表

米国国立標準技術研究所（NIST）は、「Cybersecurity Framework（CSF）」の第2.0版を公表した。CSFの第1.0版は2014年に公表され、サイバーセキュリティリスクを管理するライフサイクルの理解を提供してきた。今回の改定では、重要インフラ以外のあらゆる分野の組織に適用可能とし、また組織のガバナンスにも焦点を当てたという特徴を有する。

日米豪印首脳会合（QUAD）

（2022年5月）「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。

（2023年5月）「オープンRANセキュリティ報告書」及び「ソフトウェア・セキュリティに関する共同原則」が公表された。

2024年3月 重要インフラ安全保障法2018（SOCI法）

豪州内務省は、2024年以降の重要インフラ安全保障法2018（SOCI法）に基づくコンプライアンス規制態勢を見直すと公表した。SOCI法は、インシデント報告義務等、重要インフラ事業社に多くの義務を課しているが、事業者のコンプライアンスを効果的に向上させることを目指す。

国際連携の推進

■ サイバー空間は国境を越えて利用される領域であり、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠なため、**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を低減させる等の観点から開発途上国に対する**能力構築支援**を行うほか、国内企業のサイバーセキュリティ分野の**国際競争力向上**を図る取組も推進。

①有志国との二国間連携の強化

米英豪仏印等の有志国との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。

③ISAC*を通じた民間分野での国際連携の促進

米・EU等のISACとの連携推進、ISP向け日ASEAN情報セキュリティワークショップ等の実施。

⑤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

国際電気通信連合等における標準化活動への貢献（ITU-T SG17）（IoTセキュリティ、サイバーディフェンスセンター(CDC)、５Gセキュリテイ等）

②多国間会合を通じた有志国との連携の強化

日米豪印（Quad）上級サイバー会合、OECD/DPCデジタルセキュリティ作業部会、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。IGFにおける議論。

④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）、大洋州島しょ国への能力構築支援の試行、世界銀行との連携等。

⑥国内企業のASEAN地域等に向けた国際展開支援

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。
CDCの普及。

*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。

サイバーセキュリティ分野における国際連携（近年の実績）

■サイバー空間は国境を越えて利用される領域であり、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠なため、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貢献。
■既存の枠組みを活用し、米国をはじめとする有志国等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。近年の主な実績は以下のとおり。

1．有志国との二国間連携の強化

(1) サイバー協議
- 日英サイバー協議（2023/2）
- 日米サイバー協議（2023/5）
- 日印サイバー協議（2023/9）
- 日仏サイバー協議（2023/11）
- 日EUサイバー協議（2023/11）
- 日豪サイバー協議（2023/12）

(2) ICT政策対話
- 日EU ICT政策対話（2024/2）
- 日米デジタルエコノミー政策対話（2024/2）

2．多国間会合を通じた有志国との連携強化

(1) OECD/CDEPセキュリティ作業部会
- セキュリティ・グローバル・フォーラム（日本・OECD事務局共催）（2023/3）
- OECD/CDEPセキュリティ作業部会※（2023/3, 11）

※2024年1月より「OECD/DPCデジタルセキュリティ作業部会」に名称変更

(2) インターネットガバナンスフォーラム
- インターネットガバナンスフォーラム（2023/10）（日本ホスト）京都
  DAY 0 イベント（サイバーセキュリティ能力構築支援）

(3) QUAD上級サイバー会合
- インド会合（2023/1）
- 東京会合（2023/12）

(4) 日ASEANｻｲﾊﾞｰｾｷｭﾘﾃｨ政策会議
- ワーキンググループ会合：
  フィリピン会合（2023/2）
  ブルネイ会合（2023/5）
- 本会合：東京（2023/10）

(5) シンガポールサイバーウィーク
（2022/10）

3．ISACを通じた民間分野での国際連携の促進

(1) ISP向け日ASEAN 情報セキュリティワークショップ
- 東京開催（2023/1）
- 東京開催（2024/3）

4．インド太平洋地域の途上国に対する能力構築支援

(1) AJCCBC
- サイバーセキュリティ等に関する日ASEAN能力向上ﾌﾟﾛｸﾞﾗﾑ強化ﾌﾟﾛｼﾞｪｸﾄ開始ｾﾚﾓﾆｰ（2023/6）

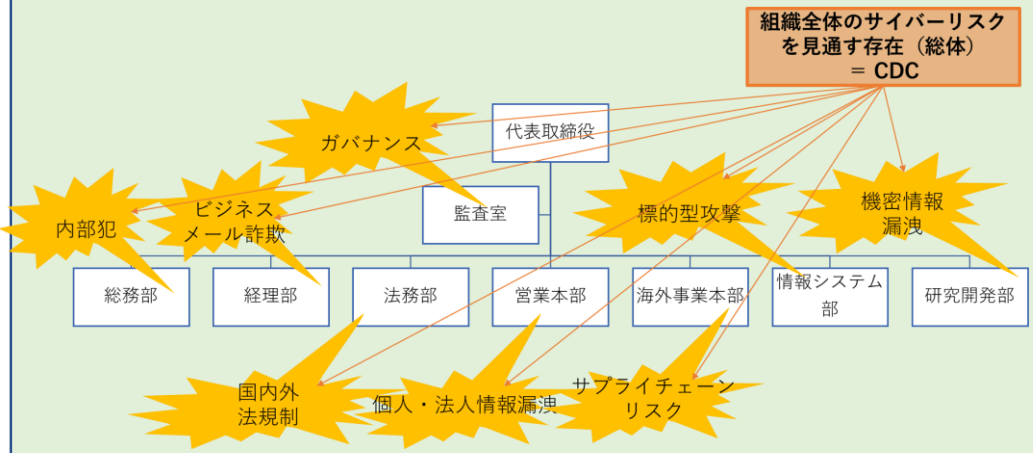
(2) 学術機関との連携
- 日ｱｼﾞｱ学術機関連携ﾜｰｸｼｮｯﾌﾟ（2024/1, 3（予定））

サイバーディフェンスセンター（CDC）について

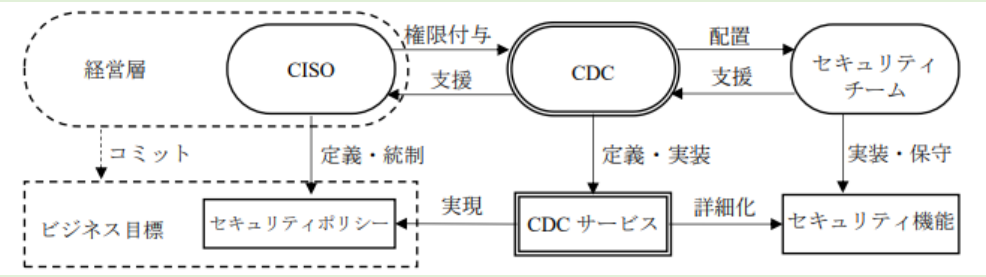
- ITUにおいて議論されていたサイバーディフェンスセンター（CDC）が、2021年10月、ITU勧告X.1060（the Framework for creation and operation of a cyber defense centre）として発行された。
- 本勧告には、日本発のサイバーセキュリティの知見として、政府や各省庁、民間セキュリティ団体の政策やノウハウが取り入れられている。
- サイバーセキュリティ体制の構築が遅れている発展途上国を対象にCDCの普及展開活動を実施することにより、サイバーセキュリティ分野における我が国の国際的なプレゼンス向上を図る。

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を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）

CDC普及展開のためのワークショップ結果概要

■ 2024年2月22日（木）、総務省支援によりITU-Tが主催して、サイバーディフェンスセンター(CDC) のフレームワークに関するにワークショップを開催。
■ ワークショップには、総務省およびITU-T関係者をはじめ、JPCERT/CC、FIRST、Google、NRD、アルジェリアテレコム、 Broadcom Europeから代表者が参加し、ITU勧告X.1060の紹介を交えて、CDCの普及展開に向けて、X.1060の導入事例や既存のサイバーセキュリティフレームワークとの協働について、情報共有や意見交換を実施した。

1．ワークショップ概要

日時･場所　　：2024年2月22日(木) 14:30-17:30、スイス･ジュネーブ ITU本部（会場参加者30名以上）
登壇者　　：総務省、ITU-T、アルジェリアテレコム、JPCERT/CC、Google、NRD、FIRST、Broadcom Europe

2．発表概要

□ 開会挨拶：

総務省より、今回のワークショップ参加者への謝意を示すとともに、
今回の議論がCDCへの理解を深め、より多くの組織がCDCを取り入れることの契機となることへの期待を示した。ITU-Tからは、ワークショップ開催及びX.1060の普及展開に尽力された方々、特に総務省の支援への感謝を述べるとともに、ITUの標準策定によりグローバルな協力関係が発展することへの期待を示した。

総務省挨拶模様

主要参加者記念撮影

□ セッション1：<u>CDCフレームワークと移行戦略</u>

アルジェリアテレコムより、当社でのCDCを活用した組織整備のケーススタディについて紹介したのち、JPCERT/CCより既存のセキュリティ組織へのX.1060のサービスメニューの適用について説明され、 NRDより、アフリカや中央アジアでのサイバーセキュリティ対策組織を立ち上げた経験について紹介があった。議論を通じて、X.1060は改訂を通してさらに改善される必要があるという点で見解が一致した。

□ セッション２：<u>サイバーセキュリティフレームワークに関する協力の強化</u>

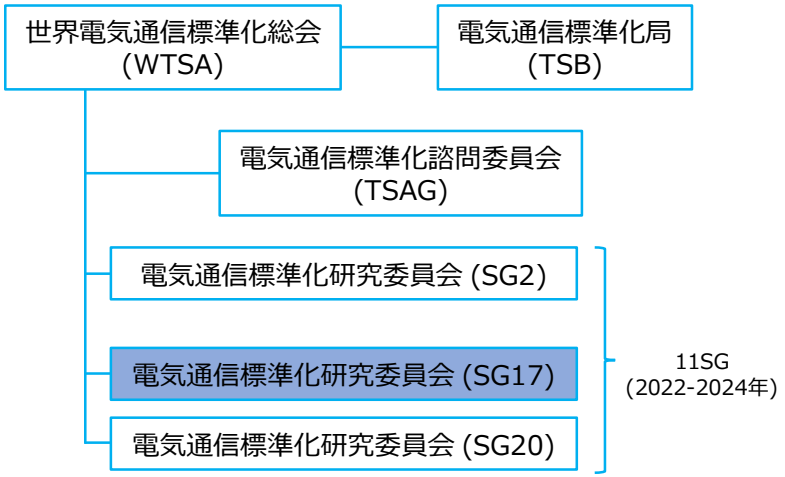
Googleより、MVSPというセキュリティに関する最小要件がアフリカ・アラブにどう活用できるかについて紹介したのち、 FIRSTより、FIRST CSIRT Service Frameworkについて説明され、Broadcom Europeより、X.1060の標準策定のエディターとして標準そのものの議論の先行きについて紹介があった。議論を通じて、既存のサイバーセキュリティフレームワークとの協働が重要であるという点で見解が一致した。

ITU-T（国際電気通信連合電気通信標準化部門）における日本の取組

- ITU（国際電気通信連合）の電気通信標準化部門（ITU-T）に設置されているSG（Study Group）のうち、「セキュリティ」を扱うSG17に参加。
- SG17において、以下の日本提案文書について勧告化に向けた議論を継続中
  - ・5Gセキュリティガイドライン（2022年8月提案） 2024年度中に勧告化見通し
  - ・IoTセキュリティガイドライン（2018年9月提案）2024年度中に勧告化見通し

ITU-Tの概要、構成

◆通信事業者間、あるいはネットワーク利用者と通信事業者の間で、ネットワークの相互接続を可能とし、エンドツーエンドで通信サービスが利用できるよう、サービス目標、技術仕様、運用の基本的規則、通信サービス料金の原則等を研究・調整し、相互運用可能な設備の通信プロトコル、技術・サービスに関する勧告を策定する機関である。



SG17課題構成（2024年2月時点）

	課題名
SG17	セキュリティ
WP1	セキュリティ戦略と調整
Q1	セキュリティ標準化戦略と連携
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
WP2	5G、IoT及びITS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
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
Q13	高度道路交通システム（ITS）セキュリティ
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
WP4	サービスとアプリケーションのセキュリティ
Q7	安全なアプリケーションサービス
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
Q14	分散型台帳技術（DLT）のセキュリティ
WP5	根源的なセキュリティ技術
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-T（国際電気通信連合電気通信標準化部門）における日本の取組

５Gセキュリティガイドライン

・2022年4月、総務省が「5Gセキュリティガイドライン第１版」を公表。
・5Gシステムのセキュリティを実際に確保するための包括的なガイダンスを提供。

（ガイドラインの主な項目）
・主要５G技術の解説
【ネットワーク仮想化、ネットワークスライシング、MEC（Multi-Access Edge Computing）等】
・脅威の分析
【一般的なセキュリティ脅威、NFVワークロードに対する脅威、RANに対する脅威、MECに対する脅威等】
・セキュリティ対策
【組織的な対策、運用管理策、技術的対策等】

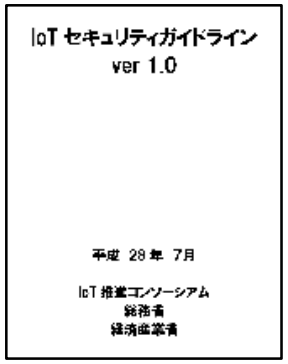
ITU-Tに対して
国際標準化に向けた検討を提案

2022年8月、ITU-T SG17において本ガイドラインをベースとして、5Gシステムのためのセキュリティ管理策に関する文書（X.5Gsec-ctrl）の勧告化が作業項目として承認され、議論を継続中。2024年度中に勧告化見通し。

IoTセキュリティガイドライン

・2016年7月、IoT推進コンソーシアム・総務省・経済産業省が「IoTセキュリティガイドラインver1.0」を公表。
・IoT機器やシステム、サービスにおけるセキュリティ確保の観点から求められる基本的な取組を提供。

IoT Acceleration Consortium
総 務 省　経済産業省



ITU-Tに対して
国際標準化に向けた検討を提案

（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（X.sc-IoT）の勧告化が作業項目として承認され、議論を継続中。2024年度中に勧告化見通し。

ISACを通じた民間分野での国際連携の促進

■ 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、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、通信分野ISAC(*)組織間における情報共有・連携を促進。

日米連携

- 2016年から日本のICT-ISACと米国のIT-ISAC間で意見交換を年１回のペースで開催。2019年にはICT-ISAC・IT-ISAC間で協力に係る覚書を締結。
- ICT-ISACとIT-ISAC間における効果的な情報共有の在り方について、日本側及び米国側関係者が議論を重ね、情報共有の自動化、共有する情報の種類、情報の活用方策等について引き続き検討。
- ICT-ISAC、IT-ISAC・Com-ISACが参加する国際連携のワークショップを2016年から開催。

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

今年度の取組

- 2024年1月31日（水）、総務省と（一社）ICT-ISACの共催により、日米欧におけるICT分野のISAC連携をテーマにワークショップを開催。（会場参加者72名）
- 日本側は総務省、ICT-ISAC、米国側は国土安全保障省（DHS/CISA）、Comm-ISAC及びIT-ISACそして欧州側はETISがオンライン参加し、日米欧の政府、ISAC組織による近年の主な取組等の紹介を交えて、ICT分野におけるサイバーセキュリティ関連の様々な取組について情報共有や意見交換を実施。

日米欧ISAC連携ワークショップの様子（2024年1月）

項目	発表概要
基調講演	IoTの視点から見たNICTにおけるサイバーセキュリティ関連の取組　等
総務省	ICTサイバーセキュリティ総合対策、NOTICE(NICT法改正)、ISAC国際連携の取組　等
ICT-ISAC	ICT-ISAC概要、大規模イベントでのサイバーセキュリティ対策の貢献　等
DHS/CISA	CISAにおけるサイバーセキュリティの取組、2024年に注力している優先課題　等
Comm-ISAC	Comm-ISAC組織概要、2024年の優先課題および具体的な取組　等
IT-ISAC	IT-ISAC組織概要、サイバー空間における現状の課題および対策　等
ETIS	ETISの成立過程および現時点での取組の紹介　等