諸外国とのサイバー分野における連携強化に関する経費

【令和５年度予算額】歳出ベース：２億円（契約ベースも同額）

１．事業概要

〇安全保障上の極めて重大な課題であるサイバー攻撃に対して、迅速かつ的確に対応するためには、我が国自身の体制強化のみならず、同盟国である米国をはじめとする諸外国と効果的に連携することが必要。

〇本事業は、上記の認識の下、米国や英国、NATO等との間で、訓練、政策的内容も含む情報共有及び人材育成に関する連携のあり方など、様々な協力分野に関する専門的、具体的な意見交換、サイバー協力を実施。

〇これらの取組を通じ、同盟国との領域横断作戦を円滑に実施するための協力及び相互運用性を高め、同盟国のみならず、一か国でも多くの国々と連携を強化する。

【米国】

・日米「２＋２」閣僚会合や日米防衛相会談の中で、サイバー分野における協力を強化することで一致

【豪州】

・ 豪国防省主催の多国間サイバー演習「サイバースキルズチャレンジ(Cyber Skills Challenge)」への参加

【NATO】

・NATO主催の多国間サイバー演習「サイバー・コアリション(Cyber Coalition)」への参加

・防衛省としてNATOサイバー防衛協力センター（CCDCOE＊）の活動に2022年10月に正式参加。
（同センターに防衛省職員を１名派遣）　（*Cooperative Cyber Defence Centre of Excellence）

・NATOCCDCOE主催の多国間サイバー演習「ロックド・シールズ（Locked Shields）」への参加

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

CCDCOEのシンボルマーク

【英、独、仏、ASEANなど】

・サイバー協議や能力構築支援を通じて、サイバー協力の取組を実施

２．論点

〇諸外国との効果的な連携手法について

①サイバー協議や諸外国とのサイバー対処訓練により、国際連携の取組をこれまで実施しているが、これまでの取組以外にも効果的な連携のあり方はあるのではないか。

②防衛力整備計画において、一国でも多くの同志国を増やすことが記載されているが、サイバー領域において、今後どのような国々に交流・協力を広げる必要があるのか。

3．ロジックモデル

アクティビティ（活動）	アウトプット（活動実績）	アウトカム（初期）	アウトカム（中期）	アウトカム（長期）
○ 米国をはじめとする諸外国とサイバー協議を実施 ○ NATOサイバー防衛協力センター（CCDCOE）主催の多国間サイバー防衛演習「ロックド・シールズ」をはじめとする、諸外国とのサイバー訓練を実施	○ 諸外国とのサイバー協議の回数 ○ 諸外国とのサイバー対処訓練の回数	○ NATOCCDCOE主催の多国間サイバー防衛演習「ロックド・シールズ２０２２」に参加 ○豪州主催の多国間サイバー演習「サイバースキルズチャレンジ（Cyber Skills Challenge）に初参加 ○ NATO主催の多国間サイバー演習「サイバー・コアリション(Cyber Coalition)」への参加 ○ 日米ITフォーラムの実施 協議や訓練への参加による連携への認識共有	○ 諸外国とのサイバー協議の回数の増加 ○ 諸外国とのサイバー対処訓練の回数の増加 米国をはじめとする諸外国との連携の強化	○ 日米共同による領域横断作戦を円滑に実施するための協力及び相互運用性を高めるための取組を一層深化 ○ 同盟国のみならず、一か国でも多くの国々と連携を強化

（参考資料）

日米サイバー防衛協力について

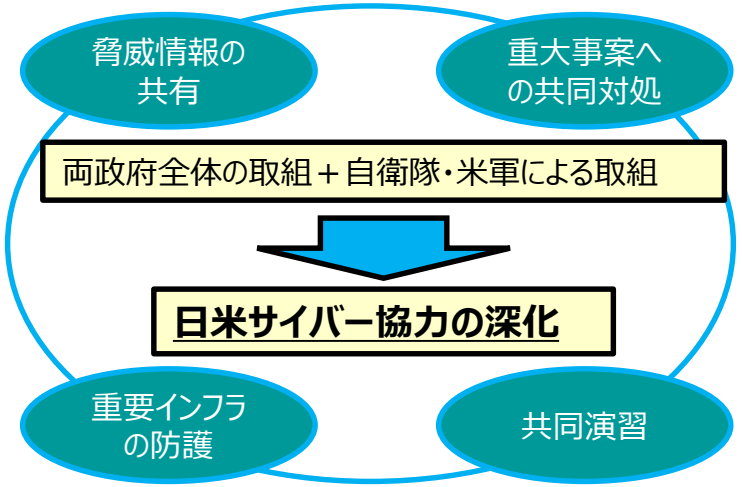
- 近年、サイバー攻撃の態様は、より一層複雑化・巧妙化・高度化。また、国境を越えるサイバー空間の脅威に対しては、国際的に連携して対処していく必要。
- サイバー攻撃は、自衛隊や米軍の任務遂行の場面において大きな阻害要因等となり得ることから、今後日米防衛協力を一層推進していく上で、サイバー空間の安定的かつ効果的な利用の確保は重要。

日米サイバー協力の主要枠組み

日米サイバー対話
（政府間の包括的協議。7回開催）

日米ITフォーラム
（防衛当局間の情報通信分野に関する協議。１５回開催）

日米サイバー防衛政策ワーキンググループ(CDPWG)
（防衛当局間の政策協議。８回開催）



日米サイバー防衛協力の主要成果

日米防衛協力のための指針（２０１５年4月）
- サイバー空間に関する協力の項を新たに設け、情報共有等、今後の日米のサイバー協力に関する方向性を記述

日米ｻｲﾊﾞｰ防衛政策ﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ(CDPWG)共同声明（２０１５年5月）
- サイバーに係る脅威認識を共有した上で、重大なサイバー事案への対処、役割・任務、情報共有、重要インフラ防護等、防衛省・国防省間における具体的な協力分野を記述。

日米「２＋２」共同発表（２０１９年４月）
- サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約第５条にいう武力攻撃に当たり得ることを確認。

日米「２＋２」共同発表（２０２３年１月）
- 閣僚は、同盟にとっての、サイバーセキュリティ及び情報保全の基盤的な重要性を強調した。閣僚は、２０２２年３月の自衛隊サイバー防衛隊の新編を歓迎し、更に高度化・常続化するサイバー脅威に対抗するため、協力を強化することで一致した。米国は、より広範な日米協力の基盤を提供することとなる、政府全体のサイバーセキュリティ政策を調整する新たな組織の設置及びリスク管理の枠組みの導入など、国家のサイバーセキュリティ態勢を強化する日本のイニシアティブを歓迎した。閣僚は、日本の防衛産業サイバーセキュリティ基準の策定に係る取組を含む、産業サイバーセキュリティ強化の進展を歓迎した。そして、閣僚は、情報保全に関する日米協議の下でのこれまでの重要な進展を強調した。

【参考】サイバー攻撃対処等を含む情報通信分野におけるその他関係国との連携

NATO

○ **日NATOサイバー防衛スタッフトークス**
- サイバー空間を巡る諸課題について相互に紹介、意見交換を実施。
- 議長：〔日側〕防衛政策局戦略企画課長 〔NATO側〕NATO新規安全保障課題局サイバー防衛課長

○ **NATO主催の多国間サイバー演習への参加**
- ２０１９年、２０２２年にNATO主催の多国間サイバー演習「サイバー・コアリション(Cyber Coalition)」に正式参加

○ **NATOサイバー防衛協力センター（CCDCOE [*1]）との協力** （*1 Cooperative Cyber Defence Centre of Excellence）
- ２０２１年、２０２２年にCCDCOE主催の多国間サイバー演習「ロックド・シールズ(Locked Shields)」に正式参加
- CCDCOE主催のサイバー紛争に関する国際会議(CyCon [*2])への参加 （*2 International Conference on Cyber Conflict）
- ２０２２年１０月、防衛省は正式に同センターの活動に参加(２０１９年３月～２０２２年３月に防衛省職員１名、２０２２年８月以降、他の防衛省職員１名を派遣中。)

欧州（２国間）

○ **防衛当局間によるサイバー協議（英国、ドイツ、フランス、エストニア）**

ASEAN

○ **日ASEANサイバーセキュリティ能力構築支援事業**

ベトナム

○ **日越ＩＴフォーラム**
- サイバーセキュリティを含む情報通信分野の取組及び技術動向に関する意見交換を実施。これまで８回開催
- 議長：〔日側〕整備計画局情報通信課長 〔越側〕国防省サイバー空間作戦司令部司令

○ **日越防衛当局間「サイバーセキュリティ分野での協力に関する覚書」（2021年１１月署名）**