サイバーディフェンス連携協議会（CDC）の設置・取組について

平成25年7月

防衛省

運用企画局・経理装備局

サイバーディフェンス連携協議会（CDC）の概要

（1）防衛省・自衛隊の活動は、電力、交通、通信といった一般の社会インフラをはじめ、装備品の開発や整備についても民間部門に依存しており、社会全般におけるサイバー空間の安定的利用の確保は、防衛省・自衛隊自身にとってもきわめて重要である。

（2）民間部門のうち特に防衛産業は、防衛省・自衛隊が継続的安定的活動を行っていく上で必要不可欠であり、防衛産業が正常に機能していることが防衛省・自衛隊がその任務を遂行していくための前提となっている。

（3）このため、防衛省・自衛隊及び防衛産業に特徴的なサイバー攻撃等に関し、双方にとって利益となるパートナーシップを確立・育成し、関係者の多様な技能・知見を活用することにより、

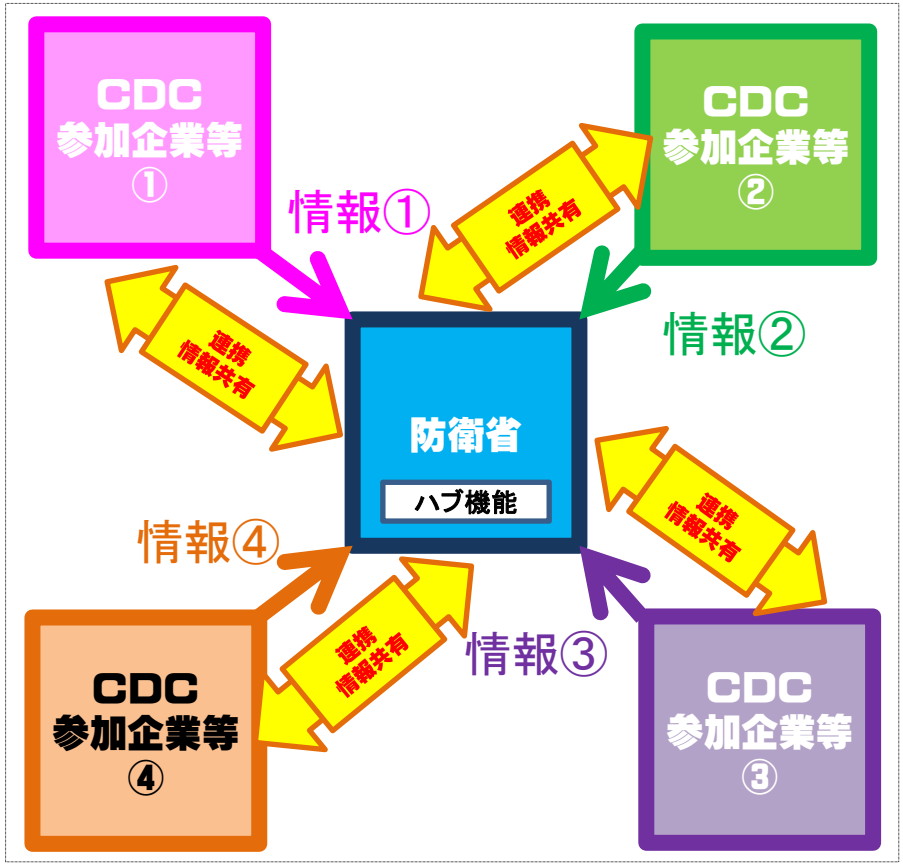
① 防衛省・自衛隊の対処能力の向上

② 防衛産業の機能・能力の維持・復旧能力の向上

③ 防衛省と防衛産業との間の信頼関係の一層の醸成

を図ることを目的とし、「サイバーディフェンス連携協議会（CDC）」（以下「CDC」（※）という。）を設置する。

（※）Cyber Defense Council



以下の取組みを通じ、防衛省と防衛産業双方のサイバー攻撃対処能力の向上を目指す。（当面は、①及び②を中心に取り組む。）

① 標的型メール攻撃等不正な通信の防止に資する情報についてCDC構成員の間で情報共有を図り、CDC構成員からの情報窃取を企図する不正な通信の防止のため、相互に連携を促進。

② 企業間において直接的には共有することが難しい当該企業に対する標的型攻撃等に係る情報について、防衛省が介在する（ハブとなる）ことにより、企業間における情報共有を可能とするとともに企業間における情報共有を促進。

③ 防衛産業に特徴のあるサイバー攻撃等についてベストプラクティスの共有を実施。

④ 防衛省・自衛隊と防衛産業とのサイバー攻撃対処能力向上のための共同訓練等を実施。

⑤ 米国等の取組事例も参考としつつ、防衛省・自衛隊と防衛産業との将来的な協力関係のあり方について検討。

サイバーディフェンス連携協議会（CDC）の概要について

１．概要

（１）防衛省・自衛隊の活動は、電力、交通、通信といった一般の社会インフラをはじめ、装備品の開発や整備についても民間部門に依存しており、社会全般におけるサイバー空間の安定的利用の確保は、防衛省・自衛隊自身にとってもきわめて重要である。

（２）民間部門のうち特に防衛産業は、防衛省・自衛隊が継続的安定的活動を行っていく上で必要不可欠であり、防衛産業が正常に機能していることが防衛省・自衛隊がその任務を遂行していくための前提となっている。

（３）このため、防衛省・自衛隊及び防衛産業に特徴的なサイバー攻撃等に関し、双方にとって利益となるパートナーシップを確立・育成し、関係者の多様な技能・知見を活用することにより、

① 防衛省・自衛隊の対処能力の向上
② 防衛産業の機能・能力の維持・復旧能力の向上
③ 防衛省と防衛産業との間の信頼関係の一層の醸成

を図ることを目的とし、「サイバーディフェンス連携協議会（CDC）」（以下「CDC」（※）という。）を設置する。

（※）**C**yber **D**efense **C**ouncil

2. 構成員

（1）防衛省・自衛隊と防衛産業との情報共有や連携関係の在り方について、防衛省・自衛隊と防衛産業のサイバーセキュリティ能力向上のための効果的なパートナーシップを構築するため、サイバーセキュリティに関心の深い防衛産業10社程度をコアメンバーとしてCDCを設置。

（2）CDCにおける取組、検討を実効性のあるものとするため、以下の理由により、具体的な参加企業名等は公開しないこととする。

① 防衛産業側の円滑な協力が得られるように取り組む必要があること
② 率直な意見交換、情報共有等を行いやすい環境を整備する必要があること
③ CDCに参加することにより企業活動に何らかの影響を及ぼさないようにする必要があること

（3）CDC構成員の変更については、上記を踏まえ、CDC全体で必要に応じ判断。

３．取組みの概要

以下の取組みを通じ、防衛省と防衛産業双方のサイバー攻撃対処能力の向上を目指す。（当面は、①及び②を中心に取り組む。）

① 標的型メール攻撃等不正な通信の防止に資する情報についてCDC構成員の間で情報共有を図り、CDC構成員からの情報窃取を企図する不正な通信の防止のため、相互に連携を促進。

② 企業間において直接的には共有することが難しい当該企業に対する標的型攻撃等に係る情報について、防衛省が介在する（ハブとなる）ことにより、企業間における情報共有を可能とするとともに企業間における情報共有を促進。

③ 防衛産業に特徴のあるサイバー攻撃等についてベストプラクティスの共有を実施。

④ 防衛省・自衛隊と防衛産業とのサイバー攻撃対処能力向上のための共同訓練等を実施。

⑤ 米国等の取組事例も参考としつつ、防衛省・自衛隊と防衛産業との将来的な協力関係のあり方について検討。

参考資料

防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて（抄）
（平成24年9月　防衛省）

３（２）民間も含めた国全体の取組への寄与

防衛省・自衛隊の活動は、電力、交通、通信といった一般の社会インフラをはじめ、装備品の開発や整備についても民間部門に依存しており、社会全般におけるサイバー空間の安定的利用の確保は、防衛省・自衛隊自身にとってもきわめて重要である。防衛省・自衛隊は、従来から、「国民を守る情報セキュリティ戦略」等に基づき、政府機関や民間企業と連携した取組を行っているが、専門的知見の提供等、内閣官房が中心となって行われる我が国全体のセキュリティレベル向上の取組に引き続き積極的に貢献するとともに、最新の攻撃手法や技術動向等の共有を図るなど防衛産業等の民間部門との協力を進めていく。

（別紙２）　具体的な取組

（２）民間も含めた国全体の取組への寄与

②民間部門を含む国全体のセキュリティ・レベルの向上への貢献

・　防衛産業等との間で最新の攻撃手法や技術動向等の共有を図る。

参考資料

サイバーセキュリティ戦略（抄）
（平成25年6月10日　情報セキュリティ政策会議）

2. 基本的な方針

（3）各主体の役割

サイバー空間に依存する多種多様な主体が、それぞれの役割を発揮しつつ、相互に連携しながら共助することにより、社会全体による動的対応力を強化していくことが必要である。

②重要インフラ事業者等の役割

我が国においてはこれまで重要インフラと位置付けられてこなかったが、当該サービス等に係る情報システムの障害等が国民生活及び社会経済活動に多大な影響を及ぶす恐れのある分野が存在する。具体的には、スマートシティやスマートタウン、ITS等の交通制御システム等の新たなネットワーク系サービスや、米国で重要インフラに含まれている防衛産業、エネルギー関連産業等である。

今後、政府において、これらの重要インフラと位置付けられていない分野における情報システムの位置づけを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について検討することとし、重要インフラの範囲等の見直しが行われた場合、新たに重要インフラ事業者等となる者においては、必要な対策を行っていくことが求められる。

3. 取組分野

（1）「強靱な」サイバー空間の構築

⑥サイバー空間の防衛

防衛関連システム以外の重要インフラ等の情報システムに対する攻撃における防衛省・自衛隊等の政府機関の役割や海外からの不正通信等に対するサイバー空間関連事業者の役割など、相互支援の在り方を含む非常時における関係機関の役割を整理し、必要な体制・機密情報等の共有システム・制度の整備等を行う。その際、個別具体的な国際法の適用についても併せて整理する。

4. 推進体制等

（1）推進体制等

政府機関や重要インフラ事業者等の関係機関間の有機的な連携のための基盤として、サイバー攻撃に関するインシデント情報等の共有を促進することが必要である。このため、攻撃者等に対して秘密とすべき情報について、既存の仕組みも活用しつつ、共有する目的、共有される情報等の内容や共有する者の範囲等に応じた秘密の保持のための枠組みを整備する。