経済産業省

資料６－３

我が国のインフラ・産業基盤・IoTソリューションの防護に向けた官民の取組について

平成28年6月

重要インフラ・産業に対するサイバー攻撃の脅威の増大

- 近年は**社会インフラを標的として物理的なダメージを与えるサイバー攻撃のリスク**が増大。
- **サイバー攻撃には、産業界に直接攻撃がなされ、大規模な停電やプラント事故のような国民の生命や財産を脅かす明確な意図を持って行われるもの**がある。
- 一方、我が国はこれまで**攻撃が顕在化した経験が少ない**ため、**事業者と政府が連携**して**「いざ」というときに備え、セキュリティ対策やスキルのレベルアップを図っていく必要**がある。

【サイバー攻撃によるインフラ障害の事例】

鉄道信号に障害発生(米国、2011年)	製鉄所の溶鉱炉損傷(ドイツ、2014年)	ウクライナの大規模停電(2015年)
鉄道会社への不正侵入により、２日間にわたって信号設備の制御に問題が発生。	標的型攻撃により、製鉄所の制御システムを不正操作。溶鉱炉が損傷。	標的型攻撃により、制御系システムを不正操作。数万世帯で、3~6時間にわたる大停電が発生。

【日本の重要インフラに対する攻撃への警鐘】

① 制御システムを狙ったサイバー攻撃

・2012年～インターネット上に水道局システムに見せかけたハニーポット（攻撃者を集めるための『おとり』システム）を設置し、調査を実施。

・攻撃者が端末を探す段階で、明らかに日本国内の水道局システムが意図的にターゲットとされ、水圧の不正な改変を行い、最後はシステム自体を不正にシャットダウンさせた。これは、水の出力を完全に停止させたのと同義。

（出典：TREND MICRO セキュリティマガジン）

② 日本の重要インフラを狙う攻撃キャンペーン

・攻撃キャンペーン「Dust Storm」の背後にいる攻撃者は、少なくとも2010年～日本や韓国、米国、欧州、その他アジア諸国の複数の組織を標的とした活動を実施。

・攻撃者が日本の企業に焦点を置き始めたのは2015年以降であり、日本の発電、オイル・天然ガス、輸送、金融、建設業界の企業ネットワークに侵入。

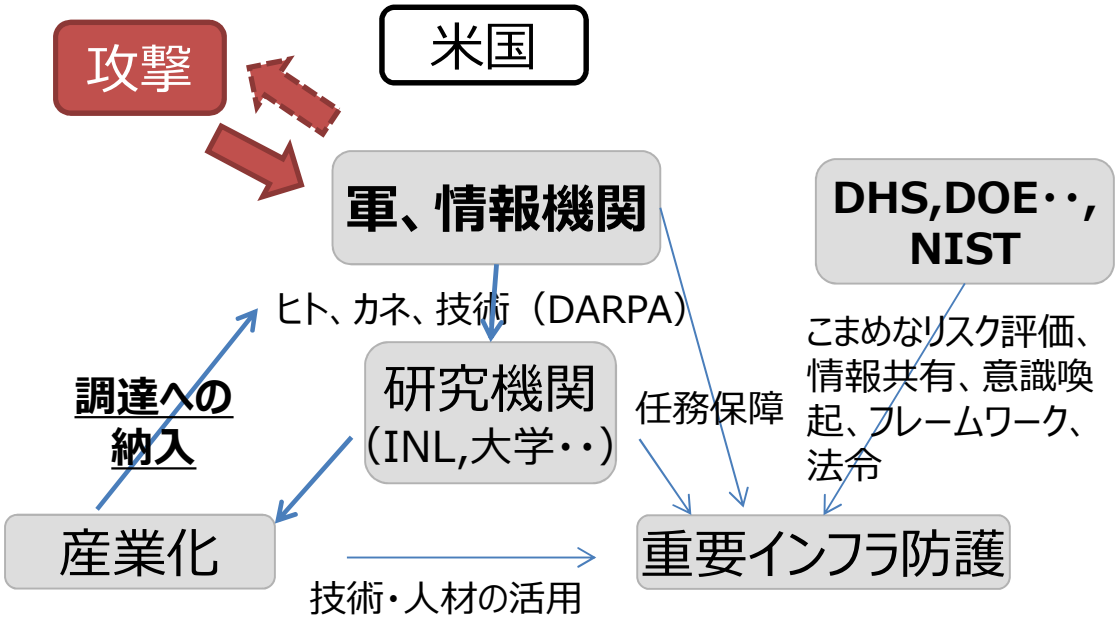
・「日本の重要インフラや資源関連の企業に対するこのような性質の攻撃は継続し、将来的には拡大し続ける」と Cylanceは結論付け。

（出典：セキュリティ会社「Cylance」の報告）

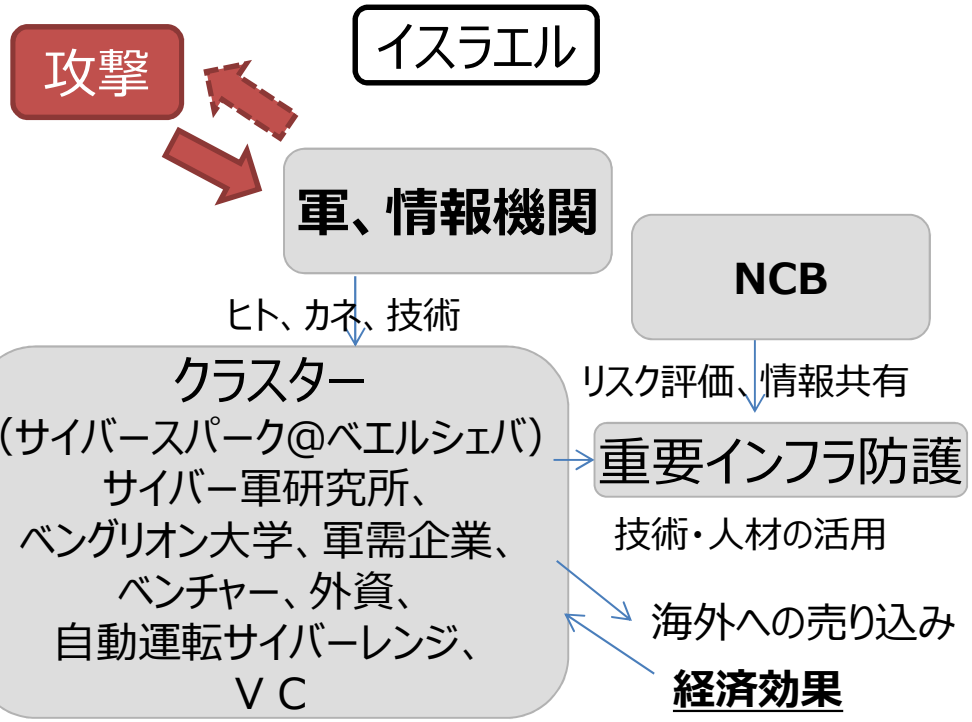
米国やイスラエルのサイバーセキュリティのエコシステム

○米国・イスラエルでは、膨大な軍事予算と、日々攻撃にさらされている**実戦経験**を通じ、**軍や情報機関のニーズに基いた極めて高度な技術と人材が養成**され、民間企業に**スピルオーバー**している。

○こうした知見は民間において**産業化**され、米国であれば**国防総省、情報機関への納入**、イスラエルであれば**グローバルマーケットへの売込み**を通じ、ヒト、カネ、技術が循環する**エコシステムが機能。**



DHS:国土安全保障省
DOE:エネルギー省
DARPA：国防高等研究計画局
NIST：アメリカ国立標準技術研究所
INL：アイダホ国立研究所



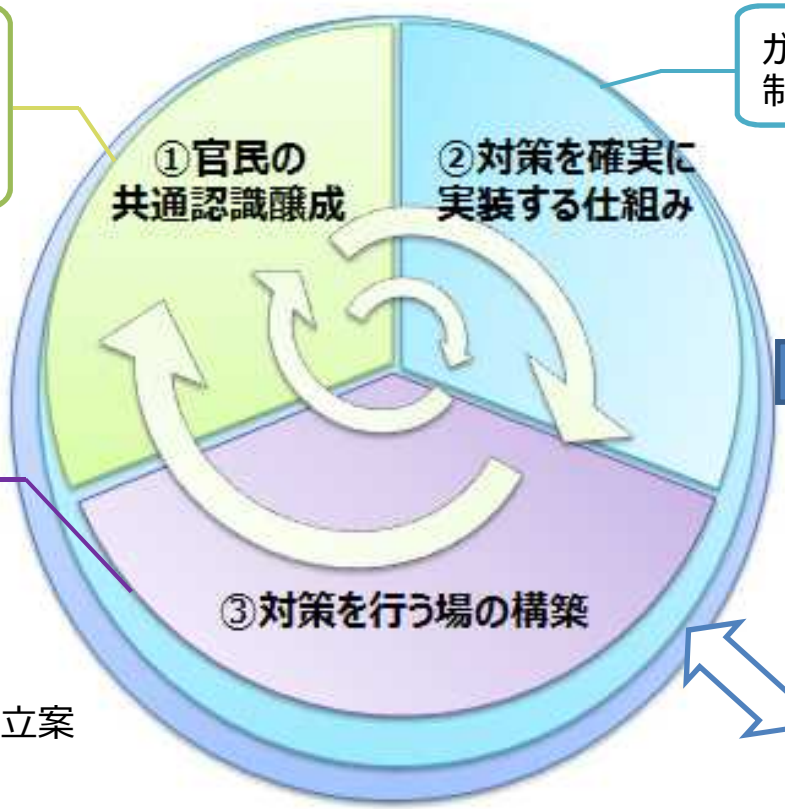
NCB：国家サイバー局

サイバーセキュリティ対策のエコシステム構築の必要性

- 今後、**ユーザー企業自身が総合的なセキュリティ戦略を立案し、対策を進めていく**ことが求められる。
- このためには、国とともに**エネルギーや自動車、素材等の基幹ユーザー産業が中心となって、セキュリティの産業化**が図られていくような**エコシステム**が必要。
- 具体的には、①国とユーザー企業が**サイバー攻撃のリスクについて共通認識**を持ち、②**対策が積極的に実装される制度**を整備し、③**国とユーザー企業が共同して対策を行うための場の構築**により、対策・技術・人材が生まれるという循環を形成していく。
- これには、サイバーセキュリティの優れた知見を持つ海外機関との連携を積極的に進めていくことも重要。

官民で国を守っていく共通認識が醸成されるよう、リスク分析・防衛力の確認や、対策のためのガイドラインを普及

ガイドライン、認証等の制度的仕組みを整備



エコシステムを通じて、総合的なセキュリティ戦略の立案・実行に必要な人材・技術を育成

優れた対策・技術・人材が輩出されるよう、基幹ユーザー産業等が参加する**「産業系サイバーセキュリティ推進機構」（仮称）**を構築

（機構の機能例）
①模擬プラントを用いた演習
②実際の制御システムの脆弱性検証・対策立案
③攻撃情報の収集・研究
④企業の経営者や担当者向けの意識喚起

国際連携
米国、イスラエル、ＡＳＥＡＮ