5　サイバーセキュリティネクサス
5　Cybersecurity Nexus

5-1　日本のサイバーセキュリティの結節点“CYNEX”
5-1　CYNEX: The Nexus of Japan's Cybersecurity

井上 大介
INOUE Daisuke

サイバーセキュリティの分野では、サイバー攻撃に関連したデータを大量に収集することと、それらデータを分析して正しく対処できる人材を育成することが重要である。しかし、我が国の多くの組織において、海外のセキュリティ技術を導入・運用する形態が主流となっており、サイバー攻撃のデータやコア技術に係る知見を国内に蓄積できないことで研究開発や人材育成が停滞し、サイバーセキュリティ自給率の低迷を招いていることが課題となっている [1]。

これまで NICT では、サイバーセキュリティ研究室がサイバー攻撃のデータを大規模収集し、ナショナルサイバートレーニングセンターが様々なセキュリティ人材育成を行ってきた。これらの膨大なデータや人材育成の知見を活用し、産学官の結節点（ネクサス）となる先端的基盤を構築することで、日本のサイバー攻撃対処能力とサイバーセキュリティ自給率を向上させることを目指した組織がサイバーセキュリティネクサス（CYNEX）である（図 1）。

In cybersecurity, collecting a huge amount of data related to cyberattacks and developing human resources and technologies to analyze data and implement appropriate measures are essential. However, many organizations in Japan have adopted and operated foreign security technologies, and the inability to accumulate know-how related to cyber attack data and core technologies has stagnated R & D and human resource development, resulting in a stagnant cyber self-sufficiency rate [1].

In the past, NICT has been collecting a huge amount of data related to cyberattacks through the Cybersecurity Laboratory and conducting various security human resource development programs through the National Cyber Training Center. The Cybersecurity Nexus (CYNEX) is an organization that aims to improve Japan's cybersecurity response capabilities and cybersecurity self-sufficiency by building a cutting-edge infrastructure that serves as a nexus, a nodal point for industry-academia-government, by utilizing such a huge amount of data and knowledge on human resource development (Figure 1).

CYNEX では 4 つのサブプロジェクト『Co-Nexus』を並行して推進している（図 2）。以下、各 Co-Nexus の活動概要を示す。

- Co-Nexus A（Accumulation & Analysis）
  NICTER、STARDUST、WarpDrive などの NICT がこれまでに開発した各種観測機構を活用し、サイバー攻撃に関連したデータを収集・蓄積する。また、国内解析者コミュニティを醸成し、共同分析の実現を目指す。
- Co-Nexus S（Security Operation & Sharing）
  解析者と機械学習エンジンの連携により複数の観測機構から得られたデータの横断分析を行い、国産の脅威情報の生成と提供を目指す。また、高度 SOC（Security Operation Center）人材育成プログラムを構築し、SOC 人材の育成拠点を形成する。
- Co-Nexus E（Evaluation）
  NICT のネットワーク環境に国産セキュリティ製品のプロトタイプを導入し、長期運用を通して機能検証と製品へのフィードバックを行い、国産セキュリティ製品の創出と普及を支援する。

図 1　CYNEX の概要

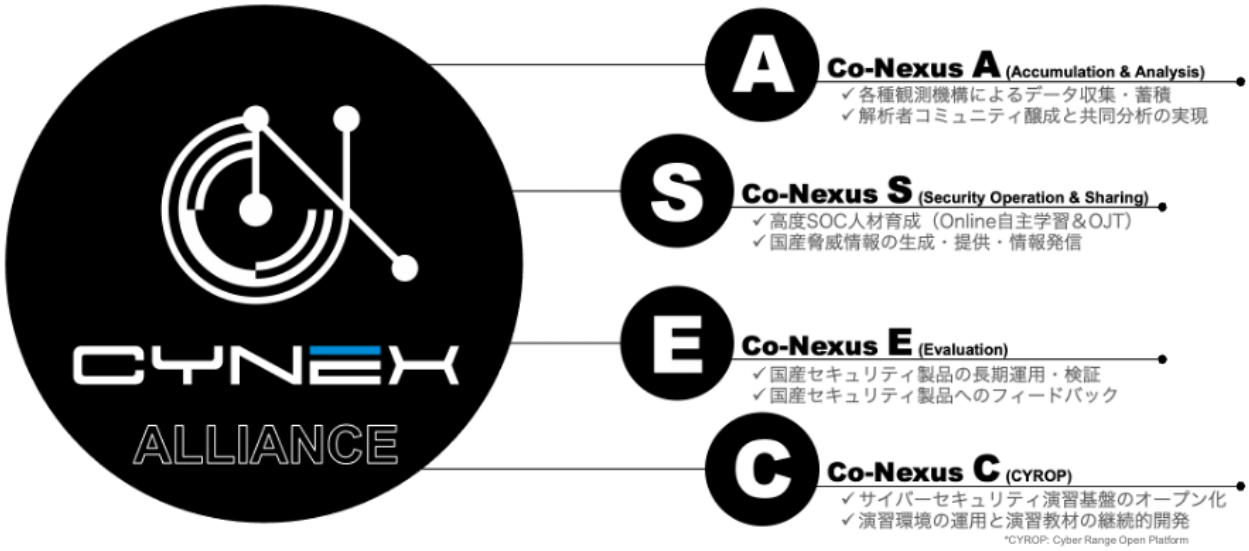

図 2　“Co-Nexus” によるプロジェクト推進

- Co-Nexus C（CYROP: Cyber Range Open Platform）
  国内におけるセキュリティ人材育成のハードルを下げるため、演習シナリオや遠隔演習システムをオープン化し、民間事業者や教育機関におけるセキュリティ人材育成事業の促進を目指す。

2023 年 10 月に国内の産学官の組織が参画する CYNEX アライアンスを発足し、CYNEX の活動を本格始動した。1 年後の 2024 年 10 月現在、参画組織数は 85 に到達し、プロジェクトは順調に進行している。以降、本研究報告では、CYNEX の 4 つの Co-Nexus の活動概要について紹介する。

【参考文献】

1　サイバーセキュリティ戦略本部研究開発戦略専門調査会，“サイバーセキュリティ研究・技術開発取組方針，” 2019.
https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai12/kenkyu_torikumi.pdf

井上 大介（いのうえ だいすけ）
サイバーセキュリティ研究所
研究所長
博士（工学）
サイバーセキュリティ、情報セキュリティ、セキュリティ可視化
【受賞歴】
2018 年　前島密賞
2016 年　産学官連携功労者表彰 総務大臣賞
2009 年　科学技術分野の文部科学大臣表彰（科学技術賞）