2024 年 10 月

JCIC コメンタリー

英国のサイバーエコシステム（英国視察報告）

JCIC 主任研究員　樋田拓也

本稿は、2024 年 5 月に英国の研究・イノベーション機構（UK Research and Innovation, UKRI）の傘下である InnovateUK※1の招へいにより視察した、同国のサイバーエコシステムに関わるコラボレーションモデルについて報告するものである。 日本から産学官含めた 10 人程度が視察団として参加した。InnovateUK は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）を通じて日本との関係を構築しており、2023 年 6 月に共同イノベーション関係をさらに深めることを目的とした 5 年間の覚書に署名している※2。

本視察を通じ、英国はサイバーエコシステムを構築するために多額の資金を投入し、産学官の連携のもとサイバーセキュリティのスタートアップの立ち上げや新しい技術の開発を行っていることが分かった。特に印象的だったのが、英国科学・イノベーション・技術省（DSIT）の資金提供を受け、Innovate UK によって実施されている”CyberASAP※3”の取り組みである。本プログラムは、学術機関のサイバーセキュリティのスタートアップを加速させるもので、11 か月の期間で実施され、最終審査まで進むと合計で 92,000 ポンド（約 1,800 万円）が支援される。このプログラムで立ち上がったスタートアップ企業のうち、実績を上げているものについては、英国政府通信本部（GCHQ）の一部である国家サイバーセキュリティセンター（NCSC）が主催するサイバーセキュリティイベント”CyberUK24”のスタートアップブースで展示および説明を行うことが認められていた。このようなイベントを行うことで、政府の取り組みが広く認知され、スタートアップの発展がさらに促進される形となっていた。これらの事例を見ると、英国におけるサイバーセキュリティ関連でのスタートアップの立ち上げが政府の支援・産学官の連携により促され、起業後も適切なサポートを受け、育成されていることが見て取れる。

日本でも 2022 年 11 月 28 日に決定された「スタートアップ育成5か年計画※4」のもと、関係省庁を含めてスタートアップ政策が推進されている。内閣府のページでも「スタートアップ創出調整連絡会議※5」の資料が公開されており、直近の取り組みを確認することができる。本政策の成果により、日本でもサイバーセキュリティに関連するスタートアップ企業が増え、日本のサイバーセキュリティの対応能力が向上することが期待される。また今後は英国を参考にし、政府が主導しサイバーセキュリティに関するスタートアップ施策の成果を周知するイベントを開催し、それを通じたさらなる日本のエコシステムンの強化も期待したい。

以下、今回の視察で議論を交わした英国のサイバーセキュリティのエコシステムに関連する取り組みおよび組織やイベントを 7 つ紹介する。

1. Digital Security by Design（DSbD）

Digital Security by Design※6（DSbD）は、英国政府が支援する取り組みで、デジタルテクノロジーを変革し、より安全な未来のためにレジリエンス能力が高い安全な基盤の構築を目指している。 ケンブリッジで行われた DSbD の会合に参加した際、英国政府が公開した National Cyber Strategy 2022 のセキュアバイデザインへの言及があった。同戦略では、脆弱性全体の 70%を占めるメモリセーフの脆弱性の問題を指摘し、問題解決のために Rust のようなメモリセーフな言語を使うことを推奨している。DSbD からは、ARM がケンブリッジ大学やケンブリッジに拠点があるスタートアップと共に研究開発した CHERI（Capability Hardware Ehchanced RISC Instructions）と呼ばれる RISC-V の新たなプロセッサの紹介があった。既にオープンソースやチップ化※7による検証が行われており、米国 FBI や CISA※8、ホワイトハウス※9も CHERI について言及している。メモリセーフな環境構築のために CHERI の導入が進むことが期待される。

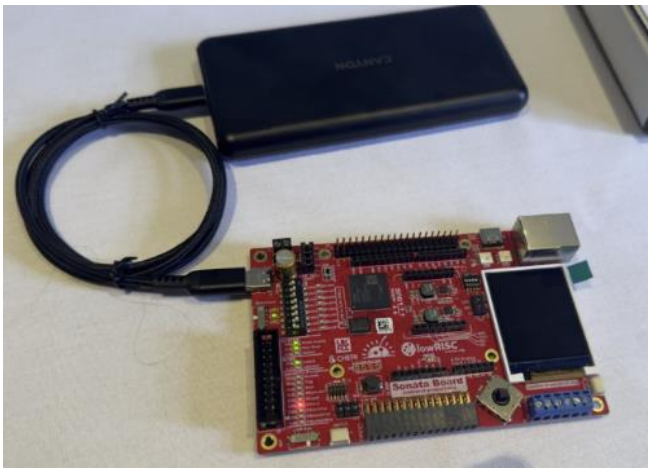


図1：CHERI を積んだボード

2. CyberUK 24

視察の一環として、バーミンガムで開催されたサイバーセキュリティに関する英国政府の主要イベントである CyberUK 24※10に参加した。最初のプログラムは、” Global Leadership Plenary – Responding to an Evolving Threat Picture”であり、グローバルリーダーシップに関するものであった。パネルディスカッションでは、英国 NCSC、米国ホワイトハウス、ドイツの情報セキュリティ庁、日本からは内閣官房副長官補で国家安全保障局次長の市川恵一氏らが登壇した。ロシアが関与するランサムウェアの脅威と中国のサイバー能力が与える英国のサイバーリスクへの影響などへ言及があり、ファイブアイズ、学術、産業との連携が必要という議論がなされた。市川氏は、アクティブサイバーディフェス、名古屋港についてのランサムウ

ェア、JAXA へのサイバー攻撃などを説明し、高度化されたサイバー攻撃に対して、検知、対応が難しくなっているため各国が協力して対応する重要性を強調した。

図2：各国政府関係者のパネルディスカッション

会場には多くの企業が出展していた。InnovateUK の調整により、NCSC が出資する Plexal が関わる複数の英国のスタートアップ企業ブースの説明を受けた。 Redflags 社のサービスは、Windows の画面上にサイバーリスクがある箇所に注意喚起を表示するアプリであり、ヒューマンリスクを低減させるために有効なツールであると考えられた。他にも、RevRng.Ai 社のサービスは AI バイナリ解析プラットフォーム、Goldilock 社は、ネットワークを遠隔から遮断するサービスを紹介し、OT のキルスイッチのように動作する仕組みを紹介していた。

図3：スタートアップ企業ブース

3. Manufacturing Technology Centre (MTC)

MTC は、2001 年から市場へ新しいコンセプトの導入を加速させるために設立された、独立の研究機関である。2022 年度は、InnovateUK から 163M ポンド(約 324 億円)の出資があり、ヘルスケア、国家安全保障、クリーンエネルギー、産業のサステナビリティなどの DX を推進している。また、 AI 製品を OT に展開するためのリスク調査や検証を政府や他のヨーロッパ諸国と連携して対応している。

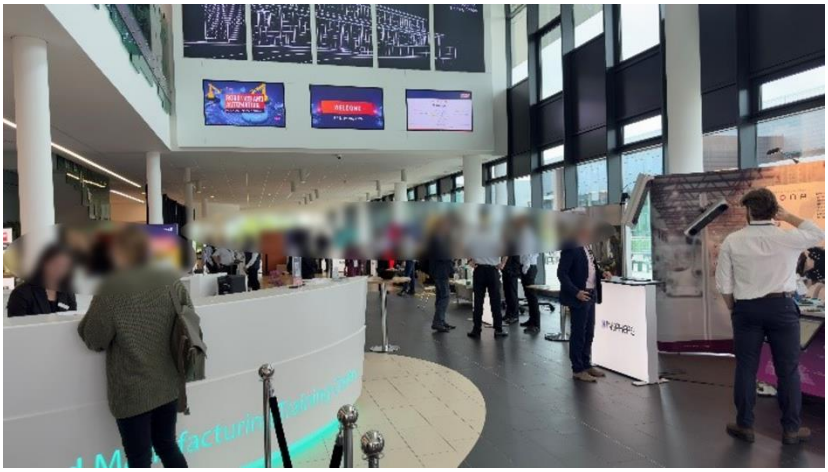


図4：MTC1 階の見学スペース

MTC の敷地内にある OT 環境を製造、検証している大規模な施設を見学した。施設内部の写真撮影は禁止であったため、画像をお見せできないのは残念であるが様々な OT 機器が展示されていた。たとえば、3D プリンタを用いたモーターの作成や、カメラで周囲の状況を撮影して画像解析してリアルタイムにフィードバックを行う作業ロボットなどである。印象的だったのは、コンテナの中に様々な設備があり、素材のカッティングからパイプを作成できる設備である。コンテナ内部にセンサーが設置され、温度や振動、機器の動きなどのデータが取得され、リアルタイムにサーバへ送信されることで状況をリモートから確認できるようになっていた。また、コンテナごと移動させることで、移動先ですぐに製品を作成できるメリットも MTC 側は強調していた。

図5：OT 環境の製造、検証を行っている施設

4. HORIBA-MIRA

HORIBA-MIRA※12は、日本に本社がある堀場製作所が 2015 年に車両開発事業やテストコースを使った車両試験領域へ事業の拡大を目指して MIRA 社を買収して設立されたものであり、2 名の日本人が出向して活動していた。HORIBA-MIRA 社の日本法人も京都にあり日英で連携して事業を行っている。自動車のサイバーセキュリティ、電気域的なレジリエンス、機能的な安全性を重要視しており、自動車に関連する様々なレギュレーション（UN 155、ISO/SAE 21434、ISO/PAS 5112）やソフトウェアのアップデート（UN156、ISO 24089）をもとに対応を行っているようである。施設内にはセルラーネットワークがあり、車のテストが実施できる”ASSURED CAV”と呼ばれる施設や自動車固有のセキュリティ問題を調査するためにレッドチーム的な活動を行う施設があった。車のシミュレーターで路面の濡れた状況を再現して様々な道路状況下で車を運転し、データを収集して開発にフィードバックできる大掛かりな設備があった。同社の社員からは、自動車に関連するは様々なデータを取得、保管しているため、過去と比べてサイバーセキュリティ対策の重要性を強く感じていると発言があった。

図6：車のテストコース（ホームページより※13より引用）

5. 英国でのイノベーションのエコシステムに関する組織

オリンピックパークに新しく作られたユニバーシティ・カレッジ・ロンドン（UCL）のキャンパスにて、英国のイノベーションに関連するエコシステム組織との会議が開催された。Catapults※14は、英国のデジタル技術を加速させるために 2013 年に設立された。InnovateUK などから出資を受け、主に 5 つのフィールド（Future Netoworks、Arfiticial Intelligence、Immersive Technology、Distributed Ledger Technology、Quantum）を対象として 35 以上のプロジェクトが稼働している。IoT Security Foundation※15 (IoTSF)からは、IoT が出始めたころはセキュリティが考えられていなかったが、2015 年付近から IoT 関連のインシデントが発生し始め、その頃に IoTSF が設立されたという説明を受けた。IoT に関するレギュレーションを調査し、ベストプラクティスの作成など各ワーキンググループに分かれて活動している。IoT に起因するサイバー攻撃は数多く発生しているため、日本との協力を呼び掛けていた。

6. British Telecom （BT）

ロンドンにある BT 社で技術の紹介と展示スペースの見学を行った。 BT のネットワークは 180 の国に展開しており、世界中のトラフィックメタデータを収集し、DNS データやハニーポット、IOC の収集と共有などを積極的に行っている。IT ハイジーンの欠如、ぜい弱性の修正や、教育の必要性や複雑で変化するレギュレーション、スキルや人材の不足について議論が交わされた。キーツールとして、「war gaming」と呼ばれる SOC チームがインシデント発生時の対応をシミュレートできるツールが紹介された。興味深かったのは、 Extended Reality（XR)技術を用いたセキュリティトレーニングの実施であった。SOC 環境構築や従業員教育として、サーバ室での作業を XR 環境で構築してトレーニングを実施するなど、XR を実際にトレーニングに使用していた。議論の後、展示スペースでのデモを見学した。3D モニタの展示では、ツールを必要とせず 3D 表示された画面の操作ができるデモが行われた。また、3D で作成されたロンドンの街並

みにセンサーを設置して活用するデモでは、iPad をかざすことで車掌の動きや人の流れなどが可視化される様子が説明された。その他には、顔認証によるセキュアなログインシステムが紹介された。ユーザ名とカメラによる撮影で認証が行われ、様々なデータにアクセス可能なシステムが紹介された。

図7：3D モニタのデモ

図8：3D で作成されたセンサーのデモ

7.　Plexal

Plexal[※16]で英国のサイバーエコシステムについて紹介があった。 Plexal は、政府、スタートアップ企業、業界とのテクノロジーのコラボレーションを通じて社会の課題解決を目指す組織である。建物内にワークスペースが用意されており、スタートアップが建物内で業務を行っていた。 Department for Science, Innovation and Technology（DSIT）科学・イノベーション・技術省[※17]は、若い世代のスキルトレーニングとして、教育部門やアカデミア、産業界、政府と連携している。その中で、CyberASAP[※3]と呼ばれる、学術機関のサイバーセキュリティのスタートアップを加速させるプログラムが紹介された。プログラムは 11 か月の期間で実施され、価値やマーケットを調査する最初のフェーズと PoC を行う 2 つのフェーズに分かれている。最初のフェーズの調査後に審査が行われ PoC に進めるかが決定される。最後まで残るのは、50%

とのことであるが、前半フェーズで 32,000 ポンド（約 600 万円）、後半フェーズで 60,000 ポンド（約 1,150 万円）が支援され、イベントなどに参加するための費用も別途支給される。このプログラムで立ち上がったスタートアップの一部は、CyberUK24 のスタートアップブースで展示されていた。　　（了）

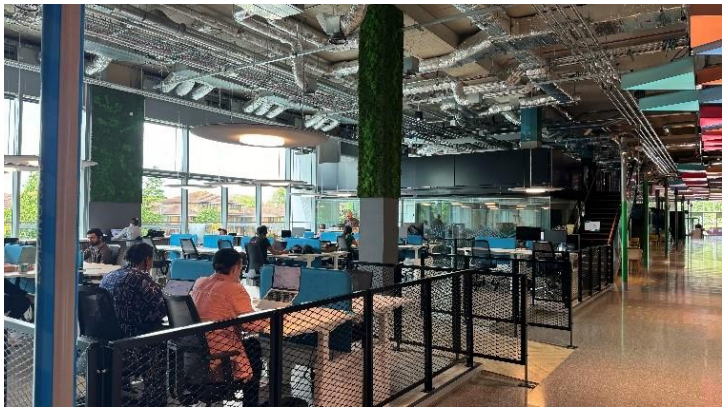


図９：スタートアップ企業に貸し出されるスペース

参考情報

※1）https://www.ukri.org/councils/innovate-uk/

※2）https://www.nedo.go.jp/ugoki/ZZ_101201.html

※3）https://iuk.ktn-uk.org/programme/cyberasap/

※4）https://www.cas.go.jp/jp/seisaku/su-portal/index.html

※5）https://www.cas.go.jp/jp/seisaku/atarashii_sihonsyugi/wgkaisai/index.html

※6）https://www.dsbd.tech/

※7）https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/cheri-risc-v.html

※8）https://media.defense.gov/2023/Dec/06/2003352724/-1/-1/0/THE-CASE-FOR-MEMORY-SAFE-ROADMAPS-TLP-CLEAR.PDF

※9）https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf

※10） https://www.cyberuk.uk/2024/about

※11） https://www.the-mtc.org/

※12） https://www.horiba-mira.com/

※13）https://www.horiba.com/jpn/company/news/detail/news/7/2015/%E8%8B%B1%E5%9B%BDmira-ltd%E3%81%AE%E4%BA%8B%E6%A5%AD%E3%82%92%E8%B2%B7%E5%8F%8E/

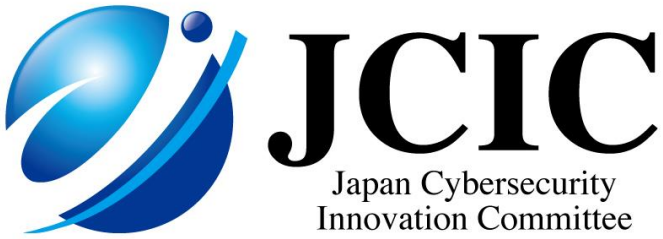
※14） https://catapult.org.uk/

※15） https://iotsecurityfoundation.org/

※16） https://www.plexal.com/

※17） https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-cyberfirst-programme/inspiring-and-equipping-future-talent-scaling-impact-of-the-cyberfirst-programme

※18） https://iuk.ktn-uk.org/programme/cyberasap/



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com