第２回 デジタル・サイバーセキュリティワーキンググループ
議事要旨

日時：令和８年４月６日（月）１４時３０分～１６時３０分

場所：東京ガーデンテラス紀尾井町４F　紀尾井カンファレンスメインルームBCD会議室
（ＷｅｂｅｘによるＷｅｂ会議も併用）

出席委員：石原委員、岩﨑委員、日下部委員、志濟委員、中谷委員、中室委員、東原委員、村上委員、横山委員、和田委員

欠席委員：井口委員（書面意見提出）

議事次第：

１．開会
２．議事
（１）官民投資ロードマップの検討状況について（事務局説明）
（２）討議
３．閉会

議事概要：

事務局より、資料１～２について説明。

以下、(2) 討議での委員との意見交換（要旨)。

＝＝
＜委員からの主なご発言＞
【官民投資ロードマップ（素案）の全体について】

- 今回の官民投資ロードマップは６本の柱が示されており、我が国としてどこに勝ち筋を見いだすのかを意識した、よく整理された全体像である。個々の技術をつなぐ面的なトータルパッケージとして整理され、研究開発から社会実装、利用拡大まで見通している点が意義深い。
- 研究・技術開発と人材育成を並行して進める必要があり、この点をロードマップの中で明確に位置づけることが重要。企業やアカデミアの連携という視点も重要であり、国・社会・企業・大学等がスピード感を持って連携して人材を育成する仕組みを研究・技術開発投資と一体で進めるべき。

- 目標に書かれている具体的な数字を達成すれば、なぜそれが成功と言えるのかという根拠が弱い。目標値と目指すべき未来社会のイメージとの間の論理的なつながりを改めて検討すべき。
- 国産にどこまでこだわるのかについて再考が必要。国内市場でのシェア獲得を目的とした国産開発への投資だけでは日本が強くなるとは言いがたく、最初からグローバルを見据えた戦略が必要。
- 全体として「国産」と「国内」の使い分けの整理が必要。全ての領域で国産を目指すのではなく、外国製品が標準を取っているものに対して無駄な投資を避け、いいものは安全保障を確立した上で幅広く活用するスタンスも重要。
- デジタル人材基盤について、細切れでしか出てこない点が気になる。デジタル人材基盤の構築・投資についても明記し、あるべき姿を描くべき。
- 地方・中小企業のデジタル変革が圧倒的に進んでいない現実があり、プロフェッショナルチームが業界をまたいで変革を同時的に推進していくような活動形態や、地方での AI 実装を手がけられる人材バンク等の構想が必要。
- 日本の強みは品質・安全・信頼にあるが、それを価格転嫁できていないことが弱点である。トラストをいかに価格に反映させるかをしっかり取り組む必要がある。また、海外でいかに稼ぐかという海外展開の視点を最初からロードマップに明確に盛り込むべき。
- インフラで培った保全・故障予兆診断、医療分野でのデータ連携・トレーサビリティ、自動運転における制御と保護の両輪による安全設計など、日本が現場・運用・責任まで含めて培ってきたシステムの品質確保の強みを生かした「フィジカル AI」が日本の勝ち筋である。
- 政府は民間に対して明確な成長ストーリーと工程を示し、産業界が投資と社会実装で応える形をつくることが重要。予見可能性を高めることで民間投資を促進し、国民が「便利になった・安心できた」という実感を持てるデジタル化を官民一体で実現すべき。
- 資本市場の視点から、日本企業が企業価値向上にデジタル・AI 活用をいかに生かしていくかが重要課題である。ロードマップ全体を通じて、AX の推進および人財育成等による組織・企業の対応力の底上げが不可欠。

【データプラットフォームについて】

- AI はデータ・AI 技術・ユースケースの三位一体で成り立つ。データがどういう意味でつながっているかというセマンティックのレイヤーが非常に重要であり、日本製の製品を育てていくことが日本のデータ主権を保つための分水嶺となる。
- 単に国内で企業を育てるだけでなく、世界と戦える企業にするという視点が企業のサステナビリティの観点から重要。
- AI-Ready 化推進に向けて、企業が扱う外に出せないデータのソブリン環境の整備が必要。国産 LLM をオンプレ・ベアメタル上で高速稼働させることや、企業が持つ匠の技を知識層として蓄えるレイヤーの構築が重要。
- 業界ごとの質の良いデータの重要性が高まる中、企業の業界の垣根を越えた産業データスペースの構築が重要。
- AI モデルは３か月で日進月歩で変わる現状を踏まえ、失敗を前向きに受け入れ、アジャイル的に改善して進めていくことが重要。

- 欧州の CBAM（炭素国境調整メカニズム）への対応など、企業間データ連携によってサプライチェーン内の CO2 削減データを自動収集するシステムの構築が可能となる。これを JCM とも組み合わせることで、脱炭素分野における産業競争力の強化につなげながら、日本の勝ち筋にしていくことが必要。企業間データ連携の推進を官民協議会で積極的に議論すべき。

【クラウド・データセンターについて】

- 「企業が扱う外部に出せないデータの AI-Ready 化推進に向けて、データ主権を維持したソブリン環境の整備が必要であり、クラウドとオンプレミスの適切な組み合わせを検討すべき。
- クラウドはあくまで手段であり、その先にある信頼・安全・安心の社会実装に軸足を置くべき。特に公共・医療・重要インフラ分野では、サイバー対策に加え、障害時のレジリエンスの確保や第三者による安全確認まで踏み込む必要がある。

【サイバーセキュリティについて】

- 我が国が目指す姿は「サイバーセキュリティ主権の実現」であり、AI 時代の競争力の源泉となるデータと AI を守るためにサイバーセキュリティ主権が必要。デジタルインフラの縦軸（ハードウェア・OS・クラウド・AI・アプリ・データ）に対して横軸として機能するサイバーセキュリティを押さえることが重要。
- 国がアンカーテナントとなり、国産サイバーセキュリティの需要を一定程度安定させる必要がある。サイバー安全保障の観点から、日本へのサイバー攻撃が割に合わないと攻撃者に思わせる体制・仕組みの構築が重要。
- 今後のアクティブサイバーディフェンスの実装でも、国産技術を一定程度活用し、日々のサイバー捜査に研究開発の要素も含めて先端技術の実装をリアルとリンクさせたイノベーションができれば、我が国の自律性を確保しながら、国内でサイバーセキュリティ製品・サービスを供給できる基盤が確立すると考える。
- 守る側だけでなく、攻める側の技術研究にも投資すべき。攻め方が分かっていないと正確な守り方ができない。セキュリティの評価も毎年更新していくようなルール化が必要。
- 外国製品を国内に合った設計・運用でうまく取り入れていく柔軟性も重要であり、それが日本らしさでもある。
- サプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）を広く周知徹底し、DX 認定・DX 銘柄のベースとなるデジタルガバナンス・コードの改訂にも盛り込むべき。業界団体（ISAC 等）のセキュリティ活動を国としても後押しし、業界横断的な訓練の実施にも広げるべき。
- 中小企業のセキュリティ強化を助成する手厚い支援があるとよい。
- AI による攻撃の高度化に対応するためには、各組織に分散している優秀な人材の知恵を集めることが重要。AI システムのセキュリティと AI を使ったセキュリティ確保の人材の垣根を取り払い、インシデントレポートも組織の垣根を取り払って収集していくことが重要。

【政府・地方公共団体の DX 基盤について】

- 国・地方公共団体の情報システム投資・DX 基盤投資はまだまだ必要であり、AI の急速な進化も踏まえ、中長期的にしっかりとした投資を行うことが重要。
- 地方自治体の DX は予算不足が深刻であり、SaaS 型・ノンカスタマイズで小規模・中規模自治体でも導入できるアプリ開発・SaaS 開発を推進すべき。
- 地方の CIO 補佐官等の DX 推進人材の報酬を上げ、若い人材が地方に興味を持てる仕組みが必要。
- 自治体向けに世の中の標準と乖離した独自システムを使わせることがないよう留意すべき。
- データ連携に当たって本人確認等データの真正性を担保する認証基盤の整備が必要であり、当面は国が主導することが求められる。
- 永住資格審査と帰化許可審査のデータ連携が進んでおらず、ワンスオンリー原則に著しく逸脱している状況の改善が必要。所管がばらばらでデータ連携できていない問題は政府全体で解決すべき課題。
- 公共分野へのデジタル投資は民間のクラウディングインを招き、経済成長に寄与するという研究もあり、しっかりとした規模で行うことが必要。
- 地方自治体のデジタル化を推進していくことが地方経済の活性化・自律性向上につながり、日本のモデルを ASEAN 展開していくことも勝ち筋の一つとなりうる。

【医療 DX について】

- 医療 DX で示されている３つの方向性（クラウドネイティブ型電子カルテの普及、大病院向けクラウドネイティブ型製品の開発、全国的なデータ連携基盤の構築）に賛同。
- 単なる電子カルテのクラウド化だけでなく、日々の診察でのデータの１次利用と研究開発・創薬への２次利用を一体的に支える基盤としてデータを位置づける必要がある。１次・２次利用を統括する法制度の整備や相互運用性に必須となる共通 ID 等の整備も必要。
- 電子カルテ周辺の各診療科システムのカスタマイズが大病院では深刻であり、周辺システムのクラウド化・SaaS 化・インターフェイスの標準化が真の標準化に不可欠。
- 医療機器のネットワーク接続点の監視・適正化や、大学病院の研究サーバーを含めたセキュリティ対策の強化が必要。
- 財源を含めた導入支援・システム開発・移行を支えるリソースの確保と、導入側へのメリットの提示が重要。医療情報の機微性を十分理解した上で、災害対策・データ連携・標準化・セキュリティまで含めて丁寧に扱うことが求められる。

【自動運転について】

- E2E への移行に伴い、従来の個別ルールへの適合性を前提とした規制からアウトカムベースの規制へ転換し、実運用データに基づいて監督していくような動的・プロアクティブな規制への対応が必要。
- 事前審査の厳格性によって実運用データが十分に集まらない状況を改善し、公的なタクシー・バスのデータを活用するなど幅広いデータ収集を推進すべき。

- OEM 中心のデータ収集だけでなく、タクシー等の公共交通を通じたデータ収集も明確に推進すべき。2028 年頃には海外勢が本格的に日本市場を取りに来ることも考えられるため、対策を進めるべき。責任分界点や保険を含めた総括的な安全の議論も同時に進めるべき。

【デジタル人材育成について】

- クラウド・セキュリティにおける人材育成は急務であり、製品よりも人を育てることが日本の国力を上げていくことにつながる。トップクラスのセキュリティ人材については才能の発掘が鍵であり、IPA の「セキュリティ・キャンプ」等を最大限に活用して才能ある人材を見いだすことが重要。
- 地方自治体では CIO 補佐官等の DX 推進人材が不足しており、報酬を上げて若い人材が地方に興味を持てる仕組みが必要。
- 一人情シス問題の解消に向けた小規模自治体への体制強化が急務。
- 研究・技術開発と人材育成を並行して進める必要があり、先端的な研究・技術領域とともに、データセンターやセキュリティ利活用など関連する基盤構築領域の人材育成も視野に入れることが求められる。
- AI が急速に進化する中、組織のカルチャーや構造を変えていくような民間への働きかけが必要。AI によって世の中が大きく変わるという認識を持った人材・組織が変革を牽引できるよう、組織構造改革も含めた取組が求められる。
- 地方での AI 実装を手がけられる人材バンクの構想や、複数の自治体・企業にまたがるプロフェッショナルチームによる共同投資・共同人材活用の仕組みが必要。

【規制改革について】

- 成長戦略で大きな官民投資があっても、出口のところで規制が障壁となり企業が社会実装できないケースが多い。AI とデジタルに関しては、技術進歩のスピードに対応できるよう、アウトカムベース・動的規制の在り方を例外的に検討すべき。
- 成長戦略の中で積極的に投資していく分野について、関係法令のどこをどれだけ動かす必要があるかを特定し、法改正・例外規定の策定も一体で戦略会議に提示するスピード感が必要。
- AI を活用した新事業に対して、何が規制上問題になるかが分かりにくい現状を改善し、先端的技術については国との間でオープンな対話ができる仕組みが必要。成長させたい分野を定め、そこに集中的に議論する場を設けるべき。

【外国人在留管理のデジタル化・データ連携について】

- 外国人が出国する際の税・社会保障等の未納分を徴収する仕組みについて、現状の対応を確認するとともに、改善を求めたい。永住資格審査（入管庁所管）と帰化許可審査（法務省所管）は共通書類が多いにもかかわらず、所管省庁が異なることでデータ連携が進んでおらず、ワンスオンリー原則に著しく逸脱している。申請者・企業双方の負担が重く、早急な改善が必要。
- 所管がばらばらでデータ連携できていない問題は、この件に限らず政府全体で見られる構造的課題であり、政府横断的に解決すべき。

＜事務局・オブザーバーからの主な発言＞

経済産業省 守谷情報経済課長

- AI-Ready 化推進に向けて、企業が扱う外に出せないデータのソブリン環境が必要との提案については、頂いた意見も踏まえながら検討を進めていきたい。
- セマンティックレイヤーが大事というご意見については、今回のロードマップ案では、AI-Ready 化という言葉を使ったが、まさに、そうしたサービスを国産で確立することに価値がある。
- データの技術的な取り組み部分はまだ黎明期であることから、最初から海外展開を視野に入れつつ、デジタルエコシステム官民協議会の議論も踏まえながら進めていく方針。

経済産業省 渡辺情報技術利用促進課長

- 企業の AX の状況を評価・可視化し、デジタルスキル標準や試験の見直しを行うことが必要。
- クラウド・データセンターは、利活用する人たちの生産性を上げる基盤として位置づけており、電力・インフラや人材の整備を通じてクラウドとデータセンターを使える環境を整えることが目的。高い信頼性・可用性が求められる分野向けの国産クラウドの必要性も認識。デジタル人材の可視化プラットフォームについてはデジタル庁と連携して検討していく方針。

経済産業省 武尾サイバーセキュリティ課長

- 海外製品への依存が高い現状において全てを国産に替えることは難しいが、製造業系の OT セキュリティ等、日本が強みを持てる分野もある。安全保障の観点でも一定程度の技術・産業基盤を国として持つ必要がある。ASEAN からの期待も踏まえ、海外展開も必要だと考える。
- 政府機関によるアンカーテナントとしての活用は重要であり、関係省庁と連携して進めていく。SCS 評価制度についても内閣官房と連携しながら広く推進していく方針。
- 攻めの技術への投資については、IPA での人材育成事業や国プロで先端技術の研究開発等の取組を進めており、御指摘も踏まえてさらに検討していく。中小企業支援についても引き続き検討していく方針。

デジタル庁 田邉参事官

- 国・地方公共団体の情報システム投資はまだまだ必要であり、AI の急速な進化も踏まえ中長期的にしっかりとした投資を行っていく。政府が率先して国産・国内技術を導入することで、潜在需要の補完と良質なデータによる学習機会の創出につなげていく。ガバメントクラウドを国・地方共通の基盤として整備し、SaaS を活用した地方展開を推進していく方針。

厚生労働省 木下参事官

- 医療 DX について、データ基盤の整備に加えた人材確保・財政支援の重要性を認識しており、ロードマップの具体化に反映していく。医療情報の特性を理解した上での標準化・セキュリティ対策を検討していく。医療データの１次・２次利用に係る法制度整備については内閣府と連携しながら議論を進めていく方針。

内閣官房 デジタル行財政改革会議事務局　鈴木参事官

- タクシー・バス・トラック等の公共交通・商用車を含めた幅広いデータ収集を推進していく。トラックも成長戦略の対象とし、また、責任分界点の再点検、保険など自動運転関連サービス、中小企業が大きなリスクなく導入できる事業モデルの構築も含めた取組を進めていく。

出入国在留管理庁 内藤次長

- 税・社会保障の未納については、令和９年３月から公共サービスメッシュを導入し関係機関から地方税の課税情報等を入手可能とする。未納が判明し納付勧奨に応じない場合は原則不許可とする運用を検討中。永住資格審査と帰化許可審査の制度間の調整については、先般の総合的対応策を受けて原則 10 年の在留要件で整合を図った。データ連携についても今後検討していく方針。

デジタル庁 松本大臣

- データセンター整備に向けた電力・通信インフラの確保が今後の制約となる。データセンター自体をこの国においてどれだけ広げていかなければならないかという視点で、電力確保やインセンティブ等を掘り下げるべき。
- 匠の技を AI に実装するフィジカル AI の観点は成長のネタになるものであり、関連するワーキンググループにも横のつながりで伝えていく。
- サイバーセキュリティの抑止効果を高めるための技術への投資については、分野横断のサイバーセキュリティの場にも伝えていく。
- 大病院の周辺システムのセキュリティについては、医療 DX の検討の中で段階的に進めていく方針。
- 地方・中小企業の共同投資によるデジタル人材確保については、サイバーセキュリティの議論でよく言及しており、分野横断の場で具体化を進めていく。
- トラックの自動運転については物流 DX の観点からも重要であり、実証の可能性を検討していく。
- ロードマップ全体として優先順位をより明確にしていくことが必要。
- AI とデジタルに関する規制改革のスピード感の問題については、成長戦略全体に関わる重要な課題として総理に伝えていく。