第１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２月３日（火）１４時００分～１６時００分

場所：経済産業省 国際会議室（オンライン（Microsoft Teams）併用）

出席委員：井口委員、石原委員、岩崎委員、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

議事次第：

１．開会
２．議事
（１）デジタル・サイバーセキュリティワーキン ググループの開催・運営
（２）事務局説明
（３）討議
３．閉会

議事概要：

事務局より、資料１～３について説明。

以下、（３）討議での委員との意見交換（要旨）。

＝＝

＜委員からの主なご発言＞

2030 年（短期）・2040 年（中長期）に目指すべき姿、実現に向けた政策の方向性

【全体について】

- 2040 年、Society 5.0 の時代が到来し、誰も取り残さないような社会を作る際に、人間が AI ロボット使ってどれだけ良い社会が作れるかを考えることが重要。そうした時代のセキュリティはどうあるべきかも議論できるといい。デジタル・サイバー領域は他 16 分野と関係が深いため接点を明確にしたほうがいい。サイバーセキュリティについてはロードマップを 16 分野で一緒に書いて、社会実装まで行い、国民が喜ぶ形にすることが重要。
- 省庁内で担当が替わっても、責任を明確化し進捗を説明するため、工程表を作成し、工程表を使って進捗を国民に見せ信頼を得るべき。
- 政策はうまくいく前提に立たず、効果検証・記録・アジャイルな修正/撤退を可能にする設計が必要。
- 国際競争力の視点で、高齢化・災害対応の経験を基に、ASEAN 等への展開も視野に（サービス/アプリケーション強化）。

- 国際比較を踏まえAI政策等をアップデートし、2040を見据えつつ短期決戦でも「今できていること/不足」を見極めアジャイルに改変・投資すべき。
- デジタル・サイバーセキュリティの取組は、企業価値向上につながり、資本市場に示すことで競争力向上にもつながる。

【クラウド・データ基盤について】

- 目指すべき姿は、2030年までに「セキュリティを担保しつつ、AI前提でクラウド上のデータを横断活用できる環境」が整い、DXが当たり前として定着。2040年はクラウドネイティブを前提に、大学等も含め国内外連携・共有が確立。医療でも標準化されたクラウドネイティブ基盤が実装され、研究・創薬にも資する環境。
- 2040年に目指すべき姿を前倒しで実現するスピードが重要。国・自治体・教育研究機関・民間が一体で基盤整備と実装を推進。量子時代を見据えた高度セキュリティのクラウド基盤、災害時も機能する通信・セキュリティ一体設計の基盤整備を提案。
- 目指すべきは、2030年は「概念・実証」ではなく、医療・公共を含む現場でAI/データ活用が定着している状況を作ることが重要。2040年は「分野ごとに閉じたDX」ではなく、「データとトラストを前提に分野横断でAIが社会基盤として機能」している状況を目指すべき。
- データ精製・ガバナンス（誰が/どのルールで使うか)・品質/責任所在を整理しないと現場実装が進まない。データ基盤を語るだけでなく、データを提供するモチベーションつまり、ユースケースの創出も重要。そしてデータ基盤とユースケースのバランスが重要であり、こうした課題は医療DXや公共分野において顕著である。データの整理、ガバナンス、セキュリティが一体となって、初めてAIによる効率化や高度化が実現できる。特にデータを精錬する際には、人間が意味を理解しながらデータを扱うことが前提となる。従来のデータは発生時に意味が固定されていたが、言葉や映像などの非構造データでは、意味を扱うレイヤーが極めて重要になる。そのため、意味処理のレイヤーを備えたデータ基盤を検討する必要がある。
- デジタルエコシステム構築の中核として、産業データスペースの整備が重要である。日本の製造業・サービス業が蓄積してきた高品質なデータは、今後のAI開発・利活用における重要な資源であり、企業・業界・国を越えて信頼性の高いデータ連携を可能にする仕組みの構築が喫緊の課題である。経団連は官民連携のもと検討を進めており、多くの企業、とりわけ中小企業の参加を促すため、実ニーズに基づくユースケースを通じてデータ連携のメリットを可視化することが重要とされている。あわせて、セキュリティを含むトラストの確保が不可欠であり、政府にはトラストサービスの体系的整備と、民間が活用しやすいガイドライン整備が求められる。さらに、国際的なデータ連携推進のため、欧州など海外データスペースとの相互運用に向けた環境整備や政府間対話の強化も重要である。
  トラストサービスの体系整備とガイドライン整備、海外データスペースとの相互運用に向けた政府間対話を提案。
- AI活用の企業側のボトルネックは未整備データ。日本企業が利用できる国産の「AI-Readyなデータ基盤」をオープンに整備することが重要。その際は、AI-Ready化の要素（構造化、意味付け、品質、ガバナンス/セキュリティ、継続改善）に加え、AIを使ってビジネスを成長させる仕組みにあたる「AI Ready Enablement」レイヤーをどう作っていくのかも

重要。また、データ連携については企業間はもちろんのこと、同様に自社内のデータ連携を進めることも重要。
- AI 活用を進めるため、「どこまでやれば良いか」が分かるガイドライン整備が AI 普及の鍵。
- 短期の話として日本の DX は上手くいっているのか。企業内・マイナンバーもそうだが、現状のプロセス改善しかしておらず、作業プロセス全体を見直していない。見直しをした上での DX 化が重要。AI を入れ、フィジカルロボットを入れていく上で、この作業プロセスの見直しは重要。
- 産業データスペースの件が中々進んでいない。競争データを抱え込むばかりではなく、それ協調データとしてデータ連携をしていくことが重要。そのために、経団連としてデータ連携のメリットがわかるような好事例の紹介や、トラスト基盤の必要性を主張している。ぜひ支援をお願いしたい。
- 産業政策として「データ蓄積」「公的データ基盤」「産業横断的デジタル連携」が効果的という研究知見を踏まえ、議論の中心に据えるべき。
- 国民本位のウェルビーイングを実現するため、社会全体のデジタルプラットフォーム基盤構築と「国産クラウドの充実強化」を期待。行政ではワンストップ/ワンスオンリーの仕上げが必要。
- データを制する者がプラットフォームを構築し、市場をロックインする「強者総取り」の構造になっている。特にサイバーセキュリティに関しては、海外プラットフォームへの依存は安全保障上の懸念に直結し、データ収集、分析、保護、活用をどのようにエコシステムとして循環させるかが重要。併せて AI 活用の基盤となる国産の LLM 技術に対する開発投資も必須。

【サイバーセキュリティについて】
- 2030 年は「個別対応から共通対応・全体最適」へ整備が進展。2040 年も共通対応・全体最適の環境が整っていることが重要。
- 企業向けに最低限の対策水準を示すガイドライン整備と、官民で「ここまでやろう」を具体化する枠組みを提案。工程表を作り、半年ごとに達成状況を国民に示すことで信頼を獲得すべき。
- AI 特有の脆弱性、AI を用いた高度攻撃に対し、人手だけでは限界。「AI には AI で」-AI 前提のセキュリティ対策が不可欠。
- 政府が「どこまでやるべきか」を示すことが道しるべになる一方、認証がチェックリスト化して自分事化を阻害しない設計が重要。
- ランサムウェアが増える中、「企業が最低限ここまでやる」水準を提示する必要、スタートアップ・大企業で連携し、官民で目標を立ち上げて進めていくことが理想。2040 年のアンビエント/ユビキタスな社会でのセキュリティの在り方も議論すべき。
- サイバーセキュリティの「自給率の低さ」は負のスパイラルによって生まれている。海外製品を利用すればデータは国外に流出し、実データは不足し国産技術が育たず、海外で日本のデータが分析・活用された製品が開発され、日本は海外製品にさらに依存する。「サイバーセキュリティ自給率」の目標値があるといい。

- サイバーセキュリティ自給率の向上に向けては、ソブリンの話だけではなく、同志国との標準整合や、懸念が認められるものは政府調達・支援プログラムから排除することも必要。サイバーセキュリティは官民総力戦で推進すべき。
- サイバーセキュリティ対策において、同志国の最先端技術を使うことで防げると思われがちだが、世界的に有名であるほど、それはリバースエンジニアリングの対象として研究されており、容易に破られてしまうリスクがある。第二の防衛ラインとして国産の技術を追加活用することが有効で、NICT が進める CYCROSS などの知見を基に、業界ごとの特性を網羅した日本独自のインテリジェンスを各企業の防御に活用できる環境を整えることは重要であり、国の役割は大きい。
- 「何を何から守るか」の定義が曖昧だと、守るべきものが守れない。設計・運用段階から必要なセキュリティレベルを定義し、国際標準（ISO/IEC 15408 等）に基づく評価の考え方も重要。
- サービス提供後の後追い対応ではなく、企画・設計時点から「守る対象/脅威/必要レベル」を定義し、国際標準等に基づく評価を織り込むべき。
- サプライチェーン全体のセキュリティが大きな課題。取引先（中小企業等）の脆弱性診断/簡易チェックなどを通じてセキュリティレディであることを認定するような仕組みが有効ではないか。
- 最近のサイバー攻撃事案を踏まえ、特に国民生活を支える重要インフラについては、業界単位で他社のバックアップを含めた BCP が出来ているか点検することも重要。
- サイバーセキュリティの強化で、厳密化、厳格化、強化していく際、中小企業が置いていかれないよう、必要な準備・事務は簡素化すべき。
- サイバーセキュリティに関して、経済産業省で検討している評価制度は、AI 時代に対応できるように今後進化させてほしい。

【分野別課題（公共分野、医療 DX・自動運転等の準公共分野）について】

- 大学は公共 DX に加え医療 DX の構築・実証の場。医療は電子カルテ等の医療データ基盤を AI 前提・セキュアでクラウドネイティブな設計へ再構築が必要。
- ワンストップ行政は海外事例も参照し、ユースケース拡大（例：車・保険などの自動連携）を進めるべき。
- 国民が「便利になった」と実感できる改革（例：死亡手続や住所変更などのワンストップ化）を提示し、国民を巻き込むべき。
- 行政は住民利便性向上が課題。コネクテッド・ワンストップ/ワンスオンリーの実現、マイナンバーカードの安心・安全運用と付加価値向上が必要。
- 自動運転の社会実装に向け、規制改革とのセット（予見性確保）が重要。政策効果検証とアジャイルな調整・撤退も提案。自動運転は実証が社会実装につながっているか疑問。世界で進むモジュール型 AI 等を踏まえ、公共ライドシェアやレベル 2 導入補助など現実的導入も検討余地。
- 医療・健康ビッグデータの活用が遅れている。電子カルテ、健診データ、レセプトなどの医療データが分散しており、データエンジニアリングのような技術や、利用範囲の制限、個人情報の取り扱いに係る国民理解をセットで紐解いていく必要がある難しい課題であるが、社会コスト削減のためにもスピード感を上げてデータ活用を推進すべき。

- 医療データの一次・二次利用を一体的に扱う新たな法制度を整備し、政府一体で医療 DX を推進すべき。

【デジタル人材の育成について】

- 基盤整備と実装を担う人材育成が急務。社会全体で AI/デジタル/セキュリティのリテラシー高度化を日常に浸透させるため、初等中等～高等教育まで一貫したリテラシー涵養、リカレント教育も重要と提案。
- 10 万人のスキルアセスメント分析から、スキル獲得だけでは行動変容が起きにくい。AI 時代にふさわしい「組織構造改革」や「AI 人的資本経営」へのアップデートが必要。
- 2026 年度までにデジタル人材を 230 万人育成するというデジタル田園都市国家構想の目標の後については、組織構造改革についても考える必要がある。育成だけでなく「使いこなして価値を出す器」（組織構造・評価制度・挑戦促進）の改革が第 2 弾として必要。AI 人的資本経営へのアップデートも提案。
- DX 人材は「戦略・ビジネスモデルに適合した人材像」を明確化し、基礎スキル＋企業固有スキルの確保・育成を見える化すべき。外部人材登用や職場環境整備（ジョブ型等）も重要。
- セキュリティ人材育成は官民挙げて進めるべき。資格（情報処理安全確保支援士）の魅力向上・リブランド、大学の講座/学部の見直しなどができないか。
- データエンジニアリングやセキュリティの人材など、ベンチャーに人が足りない。外資系企業と比較して競争力を持って採用できるようにする必要がある。加えて、大企業ーベンチャー間での人事交流など、人材の流動性を高める環境づくりが重要。
- 自治体では CIO 人材不足・「一人情シス」問題等で格差が拡大。AI 時代に適切な投資とコアコンピタンス構築が必要。
- 資本市場への見える化（開示）で DX 推進を後押し。戦略に紐づく DX 人材の明確化、外部人材登用、働く環境整備（ダイバーシティ、ジョブ型等）を提案。

＜事務局・オブザーバーからの主な発言＞

デジタル庁　田邊参事官

- マイナポータル等の基盤の上にサービス拡充を進め、出生等の手続をポータルで案内・拡充し、分かりやすい実感を提供する方針。自動運転についても関係部署と検討を進める旨。

経済産業省　守谷情報経済課長

- 企業の DX については、DX 銘柄の施策の中で、組織と AI 利活用について産業界の状況を把握しているため、この取組をさらに進め、どういった取組が必要になるか人材育成の点も含めて検討を進めていく方針。
- データと AI は一体であり、AI・半導体ワーキンググループとも連携して、データ基盤の重要性を踏まえ取り組む方針。

経済産業省　武尾サイバーセキュリティ課長

- AI トランスフォーメーションにおいて、セキュリティは表裏一体。またセキュリティの分野でも AI の活用など、新しい時代に対応していくことが必要。

- 最低限のセキュリティ対策提示や、サプライチェーン上のセキュリティ対策について、政府ではサプライチェーン上の企業が最低限実施すべきセキュリティ対策の実施事項を提示・評価する制度の構築を推進中。この仕組みを通じ、中小企業含めてサプライチェーン全体でのセキュリティ対策の強化を図りたい。
- セキュリティ分野での自給率の向上について、経済産業省では昨年３月サイバーセキュリティ分野での産業振興戦略を公表。その実現を図ることにより、セキュリティ分野の自給率向上とエコシステム構築を図っていきたい。
- 人材育成について、情報処理安全確保支援士の魅力向上は重要。資格保有者と中小企業とのマッチングなども推進のほか、若年層向けや産業界向けの人材育成も実施。各省連携、官民連携もしつつ人材育成の強化を図っていきたい。
- 開発段階からのセキュリティの考慮は、国際的にもセキュア・バイ・デザインが叫ばれており重要。当省でも IoT 製品の認証制度などの取組を進めている。リスクベースの考え方の下、各種取組を引き続き進めていきたい。

オブザーバー

- サイバー戦略（昨年末の閣議決定）に基づき、人材・国産を核としたエコシステム・中小企業/サプライチェーン等の課題を具体施策に落とし込む方針。インテリジェンス機能強化にも言及。
- 医療 DX は質向上・効率化・将来的な二次利用に資するためスピード感が必要。2030 年までに概ね全医療機関に電子カルテ導入目標。クラウドネイティブ前提、診療所の未導入解消、大病院オンプレの重いカスタマイズを踏まえた移行手順を示し改革を進める方針。
- 230 万人のデジタル人材育成目標（2022～2026）の評価を踏まえ、次の進め方を検討する旨。

デジタル庁　松本大臣

- AI-Ready データ整備は非常に重要。AI・半導体ワーキンググループの中でも議論するようにしていただきたい。
- 他の１６分野とサイバーセキュリティの連携については、分野横断的なサイバーセキュリティを検討する場もあるため、そちらで検討したい
- 17 分野の検討が出そろった段階で、デジタル庁や国家サイバー統括室（NCO）としての関与領域を整理したい。
- 国産サイバーセキュリティの強化・育成という観点は重要であり、AI、クラウドとも同じく検討を進めていきたい。
- 高齢化社会の課題を先回しして知っている我が国が、高齢化社会の DX を進めることは、ASEAN 等に展開を進めるなど巨大市場の獲得にもつながりうる点で重要。
- 中小企業のサイバーセキュリティについて。ＣＩＯやＣＡＩＯ等を業界・業態単位でまとめて誰か一人選んで雇うなど集団的に人を雇っていくこともありえるか。
- 少子化下での人材配分を再考しつつ、デジタル人材育成を大学等のアカデミアが担うことが重要。