日本成長戦略を横串で支える「デジタル・サイバーセキュリティ」

経団連デジタルエコノミー推進委員会企画部会長
SOMPOホールディングス執行役員常務グループチーフデータオフィサー
AIセーフティ・インスティテュート所長
村上明子（むらかみ あきこ）



日本成長戦略では、わが国の産業競争力強化と社会課題の解決に向けた17の戦略分野の一つとして「デジタル・サイバーセキュリティ」が位置付けられている。その具体的な方向性を検討するため、デジタル大臣と経済産業大臣を共同座長とするワーキンググループ（WG）が設置され、筆者も構成員として議論に参画している。[注1] デジタル・サイバーセキュリティは戦略分野の一つである一方、デジタルは他のあらゆる成長分野の高度化を支える共通基盤でもある。本稿では、独立した戦略分野としての施策と、各分野を横断して支える施策の両面から、WGの議論と今後の成長に向けた課題を考えたい。

デジタル・サイバーセキュリティの全体像

WGでは、デジタル・サイバーセキュリティを個別の技術施策としてではなく、産業DXや公共・準公共DXを支える一体的な基盤として捉えている。図表に示す通り、その中核にはデータ基盤、クラウド基盤、半導体基盤があり、これらをデジタル人材とサイバーセキュリティが横断的に支える。さらに、AIおよびデータ活用の拡大に伴い、クラウドやデータセンターに欠かせない電力・通信、蓄電池まで含む物理インフラの重要性も高まっている。成長戦略として重要なのは、これらを個別最適で整備するのではなく、相互に接続された基盤として強化し、産業競争力と社会課題の解決につなげることである。

デジタル・AIを支えるデータの品質と基盤

デジタル、あるいは近年注目されるAIに必須なものはデータだ。その中核には、半導体・クラウド基盤に支えられたデータ基盤がある。しかし、基盤を作ればデータが自然に集まり、活用されるというわけではない。まず、事業主側が何を実現したいのか、何が課題なのかという問いを立て、どう解決できるかの仮説を立て、必要なデータを考えることが求められる。その際、外部の知見を活用することは有効だが、何を解決すべきかという「問い」そのものまで外部に委ねてはならない。データを活用して仮説を検証し、意思決定につなげる力は、企業自身が持つべき能力である。そして、こうしたデータ活用を企業内にとどめず、企業の枠を超えて広げることで、さらに大きな価値を生み出すことができる。

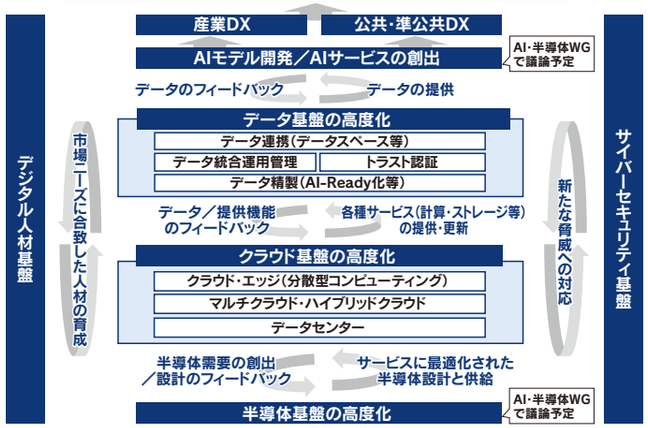
しかし、データを活用するには、その意味や形式を共有し、人やAIエージェントに対するアクセス権を適切に管理する必要がある。AIエージェントが自律的に業務を遂行する時代には、こうしたデータガバナンスの重要性は一層高まる。加えて、データは量さえあればよいわけではなく、品質も重要である。

（注1）WG詳細は下記URLを参照
https://www.digital.go.jp/councils/digital-cybersecurity

AIの品質はデータを超えることができないため、正確性や鮮度、網羅性など、目的に応じた品質管理が不可欠である。

各社とも、まだまだデータ利活用を推進している段階ではあるだろうが、データからより大きな価値を生み出すためには、企業間の連携が重要となる。そこで、2025年6月にデジタル庁と経団連は「デジタルエコシステム官民協議会」を設立し、データスペースの技術・標準やトラスト基盤の整備に加え、実際のビジネスニーズに基づくユースケース[注2]の創出を官民で進めている。

図表 デジタル・サイバーセキュリティの全体像



AI時代のサイバーセキュリティ

データやAIエージェントによって組織や企業がつながればつながるほど、「安心してつながる」ことが重要になる。デジタルがあらゆる産業の基盤となった今、サイバーセキュリティを切り離して考えることはできない。AI時代のサイバーセキュリティには、「AIを組み込んだシステムをどう守るか」という観点と、「AIによって攻撃側が高度化・高速化した際にどう対応するか」という観点の二つがある。

前者では、学習データを汚染して性能低下や誤作動を引き起こすデータポイズニングや、AIに開発者の意図しない指示を実行させるプロンプトインジェクションなど、AIに特有の攻撃を起点として、システム全体に被害が波及することへの対策が必要となる。一方、後者では、AIによって脆弱性の発見速度が飛躍的に高まることや、人間の意図しないAIが自律的に試みることが大きな脅威となっている。2026年4月、AnthropicがClaude Mythos Previewについて、その高い脆弱性発見能力と攻撃能力を公表[注3]し、一般提供を行わず、限定的な利用としたことは、AIによるサイバー攻撃能力の急速な向上を象徴する出来事となった。こうしたAI時代の新たなサイバー脅威に対し、日本政府は2026年5月、「Project YATA-Shield」[注4]を始動した。これは、AIによって脆弱性の発見や攻撃が高速化・大規模化することを見据え、官民が連携して脆弱性対応や重要インフラの防御、人材育成、防御側でのAI活用などを進め、社会全体のサイバーセキュリティを高める取り組みである。

サイバー攻撃を完全に防ぐことは不可能である。重要なのは、攻撃側よりも先に自らの脆弱性を把握し、攻撃を検知して被害を局所化するとともに、速やかに復旧して事業を継続できるようにすることである。また、AIエージェントがシステムへの広範なアクセス権や実行権限を持つようになれば、誤作動だけでなく、乗っ取りや悪意ある指示による被害も拡大し得る。攻撃側がAIを活用する以上、防御側の企業もAIを使いこなし、システムのレジリエンスを高めていかなければならない。

デジタル・データ・サイバーセキュリティは、もはやIT部門や個社だけの問題ではない。デジタルは産業を支える身体であり、データはその中を流れる血液である。また、サイバーセキュリティはコストや制約ではなく、安心してデジタルを活用し、成長するための必要条件である。

デジタル・データ・サイバーセキュリティは、成長戦略における全ての分野の共通基盤である。しかし、基盤を整備すれば終わりというわけではない。経営・事業者側がその活用にかかわる目的と責任を持つことが重要であり、そのうえで、個社では解決できない課題に官民で取り組んでいく必要がある。デジタルを「基盤整備」で終わらせず、成長につなげられるかは、私たち企業自身にほかならない。

（注2）経団連「産業データスペースの構築に向けた第2次提言」を契機に設立
https://www.digital.go.jp/policies/data_strategy
（注3）https://www.anthropic.com/research/mythos-preview
（注4）https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf