資料３

# 「サイバーセキュリティ戦略（案）」に対する意見

２０２５年10月30日（木）
三菱電機株式会社　漆間啓

「サイバーセキュリティ戦略（案）」について、**政府と経営が互いの役割を明確にして、協調しながら社会実装を加速する、**こうした観点から、**４点、コメント**します。

- **誰もが読みやすい５年不変のサイバー安全保障戦略を打ち出す**
- **政府が危機管理投資の一環としてサイバー安全保障政策を機動的に策定公表する**
- **国際的なサイバーエコステムを構築する**
- **防衛上の知見活用も含めた全政府挙げてのサイバー技術戦略を展開する**

**この４つが明確になれば、経営サイドのサイバーセキュリティ戦略がより一歩前に**出ます。**この戦略が実効性ある官民連携を実現し、社会実装加速の大きなきっかけになる**ことを期待しています。

**まず、「Ⅰ.策定の趣旨・背景」に関して、です。**

**（１）**国家関与のサイバー攻撃は、重要インフラのみならず製造業の供給網にも及びうる危機感を私は持っています。このため、まず、**この戦略案全体について大いに賛成**です。特に、「**Ⅱ.本戦略における基本的な考え方**」（P8･8-20 行目）において、「**幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上**」という**社会実装を重視**するという施策の方向性を打ち出している点に大いに共感します。

**（２）**その上で、後藤議長も前回指摘しておられたように、社会全体への実装を目指すには、サイバー空間のセキュリティ確保の重要性を皆に伝わるよう**誰にでも伝わるシンプルなナラティブとすることが重要**です。

**（３）**中小企業の方々含め多様な人々にメッセージを伝えるため、**この戦略の要点をよりわかりやすい言葉でまとめた解説を作成し、この戦略と一緒に公表**することが必要だと考えます。我々は、これからパートナーのサプライヤーの方々にサイバー対策を共に実装する働きかけを加速します。その際に、こうした**戦略の意図や背景につき具体例を挙げながら示した解説**があれば、非常に助かります。

**２点目は、Ⅱの「１.確保すべきサイバー空間のあり方及び基本原則」に関して、です。**

**（１）** 原案では、「基本原則」で**「国がこれまで以上に積極的な役割」**を果たし、対策を強化するとコミットしている点（P4・4 行目）に賛成です。多くの中小企業がセキュリティを**実装するにはコストの壁**があり、**国の支援やガイドラインが不可欠**だからです。特に **OT セキュリティ対策**については、大企業においても未だ十分な対策がされていません。サプライチェーン全体での OT セキュリティ実装に向けては、サプライチェーンを構成する中小企業の参画も不可欠であり、OT セキュリティの**実装加速のための予算面での支援やガイドラインなど国の強い後押しが必要**です。

**（２）** こうした問題意識に立って、**強調したいポイントは２つ**です。

**一点目**ですが、政府のコミットメントが明確であればあるほど、経営サイドもサイバー戦略を経営戦略として位置づける動きに弾みが付きます。

**高市総理大臣は所信表明演説**の中で、成長戦略の肝を**「危機管理投資」**と定義し、**サイバーセキュリティを含む戦略分野**に対して、「大胆な投資促進、国際展開支援、人材育成、スタートアップ振興、研究開発、産学連携、国際標準化といった**多角的な観点からの総合支援策を講ずる**ことで、**官民の積極投資を引き出す」**と宣言しました。これは本戦略の考え方とも合致します。この**危機管理投資への総合的支援策により官民の投資を引き出すとした方針を踏まえ、本戦略においても政府のコミットメントをより明確にすべき**です。

**二点目**ですが、原案では、政府の役割として、**地方公共団体や大学に対しては「支援」**(P.27・16 行目及び P.28・9 行目)**と明記**されています。しかし、**中小企業などサプライチェーンを構成するプレイヤーに対しては「支援」ではなく、「普及啓発」**(P.28・26 行目)**、「制度構築を推進」**(P.28・33 行目)**、「環境整備」**(P.29・9 行目)**、「施策を一層強化」**(P.30・2 行目)**といった表現にとどまっています。**そこで、「自助・共助・公助」のうちの「公助」(P.30・14-19 行目)として、**政府がサプライチェーン全体を支える中小企業等に対しても「支援する」と明確に力強く宣言すべき**と考えます。

**（３）** ５ 年不変の「戦略」を示す。ここにとどまらず、国は例えば戦略の行動計画や骨太の方針などを駆使して力強く「政策」にもコミットする。これを受け、企業が経営戦略をより具体化する。

この**「官のコミット・民のコミットの好循環」が、社会実装加速のカギになります。**是非、**国は、政策面でも前面に出るという方針をこの戦略で打ち出して頂きたいと考えます。**

**３点目は、「Ⅲ.目的達成のための施策」で展開している「エコシステム」に関して、です。**

（１（２）の官民連携エコシステム、１（３）の国際連携推進、３の人材・技術のエコシステム）

**（１）**人材・技術の強化においても、日本国内のリソースだけでは限界があります。やはり、**安全保障の価値観を共有する国々と、政府、企業、研究機関、人材の国際的な交流を通じて、オープンな開発体制を築く**必要があります。**原案は国内から国際へというストーリーですが、これがより鮮明になるように工夫を**お願いします。

**（２）**また、これからは、**サイバー領域でのクリアランスホルダー**が日本でも生まれます。当社も政府の声がけがあれば即応できる体制をすでに整備しています。こうしたクリアランスホルダーは、**国際的なクリアランスホルダー限定のコミュニティに参加することも可能**です。ですので、**クリアランスホルダーの国際的な活躍の視点も是非考慮してもらえると有効**だと考えます。

**（３）**これにより、経営層から実務層に至るまで、官民の専門家がグローバルなサイバーセキュリティコミュニティに参画し、**グローバルなエコシステムの一員となる道が開ければ、人材・技術が大いに高度化**します。是非、検討をお願いします。

**最後４点目は、Ⅲの３「（３）先端技術に対する対応・取組」**に関して、です。

**（１）**ここではAIやPQC（耐量子計算機暗号）、QKD（量子暗号通信）が事例として明示されています。この点は賛成なのですが、私は、この２つの事例を挙げた背景にある、大量の情報を高速処理する技術革新が日進月歩で生じていて、こうした**情報処理技術のイノベーションが攻撃を高度化し続けているトレンド**に目を向けるべきだと考えます。

**（２）**だとすると、ここでは、**「サイバーセキュリティ関連技術の開発を加速する」という方針をまず述べた上で、以降に典型例として①AI②PQC・QKD に関する取組みを記載**してはどうかと考えます。

**（３）**また、**サイバー関連の開発においては、防衛分野の知見を活用**することが極めて重要です。先端技術領域ではデュアルユース技術が非常に重要であり、**防衛分野のサイバー技術は社会実装にも十分応用可能**と考えます。ですので、**総務省や経産省が担う民生用技術の開発にとどまらず、防衛関連プロジェクトで培われた高度なサイバー技術にも着目し、その民生展開を支援するという方針を明確に**することを期待します。

以上