資料３

サイバーセキュリティ専門家会議・第４回会合向け意見
～サイバーセキュリティ戦略の具体化に向けて～

2026 年 2 月 20 日(金)
三菱電機株式会社 漆間啓

昨年 12 月の「サイバーセキュリティ戦略」の閣議決定を受け、産業全体のレジリエンス向上に向けた具体的アクションプランの策定、とりわけ中小企業を含むサプライチェーン全体のサイバー対策・防御力強化が喫緊の課題。

産業全体のサイバー防御力は、制度・費用・人材の三位一体で、官民が協働して早期に整備を実行していくことが求められる。スピード感を持って、打ち手を具体化する必要あり、以下 3 点を提言したい。

1. OT セキュリティに関するガイドラインの整備

実効性のあるサイバー攻撃の検知の仕組み導入・体制構築に関するガイドラインの充実化が必要。現状の製造業向けガイドライン[*1]では、例えば次の観点からの記載が不十分：①IT/OT の包括的な監視や連携の体制構築、②サプライチェーン上のベンダーとの組織的連携を実現する契約や教育、③IT システムのインシデント発生時に OT システムが独立的に動作を継続するための体制・仕組み。

CPSF（サイバー・フィジカル・セキュリティ・フレームワーク、2019 年 4 月策定）を改定し、産業横断の共通基準を示すべき。

2. 費用負担の仕組み整備（価格転嫁＋政策支援）

サプライチェーン全体の防御力の底上げには、一層の対策が必要な分野（中小企業、地方自治体、大学等、医療分野等）を含む対策強化が不可欠。ただし、OT セキュリティ対策の導入・維持には相応の費用負担を要するため、法人単位の自助努力に委ねるだけでは対策が進まない。サプライチェーン上での価格転嫁の仕組みと、政府による補助金の仕組みを組み合わせた制度設計が必要。

3. 人材の確保・育成に向けたコミュニティ構築

サイバーセキュリティ人材フレームワークの整備と活用促進によるキャリアパスの可視化に加え、高度人材へのインセンティブを高める観点からも、グローバルなエコシステムの中で活躍できる環境づくりが必要。また、これらの人材に対する持続的な倫理教育の仕組みづくりが必要。直近の取り組みとして、クリアランス制度を活用し、サイバー領域での官民のクリアランスホルダーのコミュニティ構築を急ぐべき。クリアランスホルダーのグローバルネットワーク形成を通じて、高度人材が更にスキルを磨き、その人材層を厚くするための自律的な仕組みを早期に確立すべき。

以上

*1 「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」等