産業横断サイバーセキュリティ検討会の取り組み

サイバーリスク情報センター 産業横断サイバーセキュリティ検討会（CRIC CSF）第6期会長
全日本空輸デジタル変革室専門部長
和田昭弘（わだ あきひろ）

２０１５年６月、重要インフラ分野を中心とする主要企業のイニシアティブにより「産業横断サイバーセキュリティ人材育成検討会」が発足した。本検討会は、産業界が連携して企業の特性や役割に応じた人材を育成することを目的に、東京２０２０オリンピック・パラリンピック競技大会に向けて活動を展開してきた。その後も、産業界を取り巻くサイバー脅威は複雑化し続けていたため、２０２０年10月に組織名称を「産業横断サイバーセキュリティ検討会」へと変更した。現在は人材育成のみならず、産業界全体のサイバーセキュリティ体制の強化を目指して、主に次のような活動を推進している。

サプライチェーン全体の防御力の底上げ

近年のサイバー攻撃は、セキュリティ対策が強固な大手企業を直接狙うのではなく、中小企業を含むサプライチェーン上の弱点となり得る部分を狙う手法が増加している。当検討会では、産業界が一体となってこうした脅威に立ち向かうべく、次のような取り組みを主導している。

・CRIC SC3との連携

中小企業を含む産業界全体でのサイバーセキュリティ対策を進める「サイバーリスク情報センター サプライチェーン・サイバーセキュリティ・コンソーシアム（CRIC SC3）」と密接に連携し、実効性の高い提言活動や会員企業への支援策を展開している。具体的には、中小企業を含む社会全体のサイバーセキュリティ水準の底上げを図るためのベースラインの設定に取り組んでいる。その一環として、日本自動車工業会等との連携のもと、今後運用開始が予定されている「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」に関する基準づくりに参画してきた。制度設計にあたっては、下請企業に対して過度なセキュリティ対策やコスト負担が求められることのないよう、「パートナーシップ」の観点から関係省庁に働きかけを行った。

・コミュニティによる情報共有

一企業では収集が困難な法令動向や実務上の課題解決策を共有する勉強会を開催している。例えば、EUの各種法令（一般データ保護規則〈GDPR〉、ネットワーク・情報システムの安全に関する指令〈NIS2〉等）や中国のサイバーセキュリティ法など、各国・地域における最新のサイバー関連法規制への対応や、ランサムウエア被害発生時の交渉の是非といった実務上の重要論点について、専門家を招聘（しょうへい）して勉強会を実施している。

会員企業間でのベストプラクティス共有は、各社の迅速な課題解決に寄与するものである。

・政府への働きかけ

社会全体のサイバーレジリエンス強化に向け、国家サイバー統括室（NCO）や経済産業省等の政府機関における様々な委員会・ワーキンググループ等に参加し、産業界（特にセキュリティサービスのユーザー企業や中小企業）の意見が政策に反映されるよう、働きかけを行っている。

経営層の意識改革と組織体制の強化

企業の経営層がサイバーリスクを「ビジネスリスク」として捉え、経営判断に組み込むための基盤づくりを支援している。

図表 産業横断サイバーセキュリティ検討会 活動のスコープ

サプライチェーン・サイバーセキュリティ
- ✓会員企業ごとにサプライチェーンが異なる産業横断の特徴を活かしたサイバーセキュリティの検討
- ✓調達先や販売・提供先が国内外に広がる事業展開を前提としたサイバーセキュリティの検討

重要インフラ事業者のサイバーセキュリティ
- ✓省庁等による産業界への要求を確認し、グループガバナンスおよびサプライチェーンの観点を踏まえた効率的なセキュリティ運用に関する情報共有
- ✓重要インフラ事業者として求められるサイバーセキュリティとデジタルトランスフォーメーション（DX）に求められるサイバーセキュリティの共通項目や差異についての意見交換

経済安全保障および各国サイバーセキュリティ動向
- ✓会員企業の約半数は、経済安全保障推進法第50条第１項および第２項の規定に基づく特定社会基盤事業者であることから、法人組織としての実施事項および対応実務に関する情報共有
- ✓米国、欧州、中国等におけるサイバーセキュリティ関連法規制が実務レベルで運用されている現状に対して、外部有識者を招聘した情報収集の機会の定期開催

ユーザー企業の組織と事業を守るためのサイバーセキュリティ
- ✓上記、様々なセキュリティ課題に対して、セキュリティ統括機能のあり方を再整理し、ユーザー企業におけるサイバーセキュリティ人材が活躍できる環境の整備に関する情報発信を行う
- ✓省庁が設置する各種委員会への参画、産学官連携による検討への参加ならびに改善に向けた提言等を行う

・「セキュリティ経営者サミット」の開催

企業の取締役・執行役員層および省庁幹部が集う情報交換の場として「セキュリティ経営者サミット」を、経団連との共催により毎年度開催している。経営層が自らリスク対策を議論する当検討会ならではの取り組みとして、参加企業から高い評価を得ている。２０２５年11月の同サミットでは、「共助から共創へ――進化するサプライチェーン・サイバーセキュリティ」をテーマに掲げた。これは、２０２３年度の同サミットで「サプライチェーン・サイバーセキュリティ」を取り上げて以降の環境変化を踏まえ、従来の「共助」を前提とした連携から一歩進み、企業や業界の垣根を越えてそれぞれの立場や役割を相互に認識しながら、「共創」へと深化させるための実効ある協調モデルの構築について議論を深めたものである。

・「セキュリティ統括室構築・運用キット」の提供

組織としてのレジリエンス力を高めるため、サイバーセキュリティ統括機能のサポート等に特化した運用キットを公表している。このキットは、概要編、統括室編、統括人材編で構成しており、概要編では、セキュリティ統括室の考え方・全体像をまとめている。また、統括室編では、ユーザー企業におけるセキュリティ組織体制のあり方を、「委員会型」「CSIRT（セキュリティ・インシデント対応チーム）型」「専任組織型」に３分類し、各企業の組織体制に応じた構築ステップを可視化できるようにしている。企業のセキュリティ体制に関する体制構築・運用改善およびアセスメントの参考として、ユーザー企業に活用されることを期待している。

次世代のセキュリティ人材の育成

複雑化するグローバル・サプライチェーンや、生成AI、クラウド移行といった技術変革に対応できる実務家の育成に取り組んでいる。

・Cybersecurity Governance Leadership Academy（CGLA）の運営

会員企業の実務家が持つ知見を凝縮し、次世代幹部人材の育成を目的とした標記の研修プログラムを、２０２５年10月より開講し、運営している。既存の教育プログラムに多い「専門技術者養成」ではなく、ユーザー企業における「セキュリティ統括」に必要な能力・知識・思考法に特化したカリキュラムが特徴である。

・人材定義の継続的アップデート

グローバルな法令遵守や技術変化に合わせた「人材定義リファレンス」の改訂を推進している。「人材定義リファレンス」とは、サイバーセキュリティ対策機能を実現する業務、さらにそれを担う各種役割（担当）ごとの要求知識と業務区分を整理したものである。現在、企業単体のみならず、サプライチェーン全体を俯瞰（ふかん）して指揮を執れる人材要件の明確化を進めている。

これからも当検討会は、政府や経団連と連携して、産業界全体のサイバーレジリエンス向上に寄与していく。