

時下ますます御清祥のこととお慶び申し上げます。

本年1月以降、国内の複数の企業が高度なサイバー攻撃を受けていたことが明らかとなり、また、サイバー攻撃により、企業情報が流出した可能性がある事例も続いています。

経済産業省は、こうした状況を重く受け止め、6月12日に「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書」¹を公表し、大企業から中小企業まで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化・高度化していることを踏まえ、昨今のサイバー攻撃の特徴や具体的事例を整理するとともに、今後の取組の方向性を取りまとめました。

企業が担うべき責任は自らの事業継続の確保に留まりません。サプライチェーンのセキュリティを確保する責任や、企業が負っている社会的な責任、例えば安全保障環境に大きな影響を与える可能性があるため適切な管理が法令で求められている機微技術情報の管理責任など、様々なものが考えられます。

本報告書では、こうした責任を果たすために企業が取るべきアクションとして、1) サプライチェーンを共有する企業間における高密度な情報共有、2) 機微技術情報の流出懸念がある場合の報告、3) 多数の関係者に影響するおそれがある場合の公表の3つを提示しています。同時に、中小企業を含めたサプライチェーン全体のサイバーセキュリティ対策の強化のために、中小企業のサイバーセキュリティ対策の取組の可視化を検討していく旨も提示しています。

この度、こうした取組を推進していくため、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的とした「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 (SC3)」が設立されます。

本コンソーシアムは、産業界主導の取組として、幅広い業界団体や個社に参加いただき、サプライチェーン全体のサイバーセキュリティ対策強化のための取組の検討・推進を行っていただきたいと考えておりますところ、ぜひ加入をご検討いただければ幸いです。

コンソーシアム設立は令和2年11月1日を予定しております。設立までに御加入いただける場合には、お手数ですが、10月30日(金)までに、後ほど送付させていただく「サプライチェーン・サイバーセキュリティ・コンソーシアム入会申込書」にて御連絡を賜れば幸いです。(恐れ入りますが、入会申込書の送付は10月中旬を予定しております。)

なお、本コンソーシアムの設立にあたりまして、本年11月19日(木)に設立総会を開催させていただき予定としております。総会への御出席希望につきましては、コンソーシアム入会申込書にて、あわせてご登録賜りますと幸いです。よろしくごお願い申し上げます。

¹ 「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書」