講演レポート

産業分野におけるサイバーセキュリティ政策

～「Society5.0」において必要なセキュリティ対策～

経済産業省　商務情報政策局
サイバーセキュリティ課長　　奥家　敏和　氏

■サイバー攻撃の変化に合わせた施策の重要性

現在、サイバー空間では水平的に攻撃範囲が拡大しており、さらに垂直的に深部まで被害が波及する攻撃が行われているという認識にもとづいて、政策立案を行っている。

水平的脅威の拡大例としては、2018 年に発生した ASUS 社端末におけるアップデート機能を悪用した攻撃が挙げられる。これは、ASUS のアップデートサーバーが攻撃され、そこから各端末に配布されたアップデートファイルを介して数十万台がマルウェアに感染、さらに攻撃では感染端末の MAC アドレスから標的とする端末のみを特定しマルウェアを作動、C&C サーバと通信させた。このような攻撃が、1 つのシステムに多くの端末が接続する 5G、IoT において行われた場合、一体どのような対処ができるのか、という問題意識を持っている。

また、クラウドに関して、昨年特に相談が多かったのがクラウドサービス上での情報漏えいである。これは、クラウドサービサー側の問題よりもデフォルト設定を把握しないままシステム構築を進めたことが原因の場合が多く、利用開始段階でリスクの把握と対策を十分確認することが必要となる。逆に、クラウドサービス側が原因のケースでは、システム自体の脆弱性を攻撃されており、結果としてサービス提供終了となった。ただし、一般的にレガシーなオンプレミスよりもセキュリティ対策に十分な投資をしているクラウドサービスの方が安全性は高いと考えられるので、クラウドサービス利用を怖がるのではなく、クラウドサービスならではのリスクと対策を考えて利用してほしい。攻撃は私たちの身の回りで起きるのではなく、私たちに影響を及ぼせるところであればどこからでも仕掛けられる。

垂直的脅威に関しては、以前はサイバー攻撃＝TCP/IP であり、産業用・制御用プロトコルには及ばないという話も聞かれたが、長期的に国家レベルで費用も時間もかけて行われる攻撃に対し、プロトコルが異なるからという話は意味を

なさない。2016 年にウクライナ停電を引き起こした攻撃では、IT 系システムから最終的には重要インフラまでサイバー空間での攻撃のみで停電を発生させたと言われている。これまでの通説を過信せず、今現在の状況を確認し、必要な対策を取ることが重要となる。

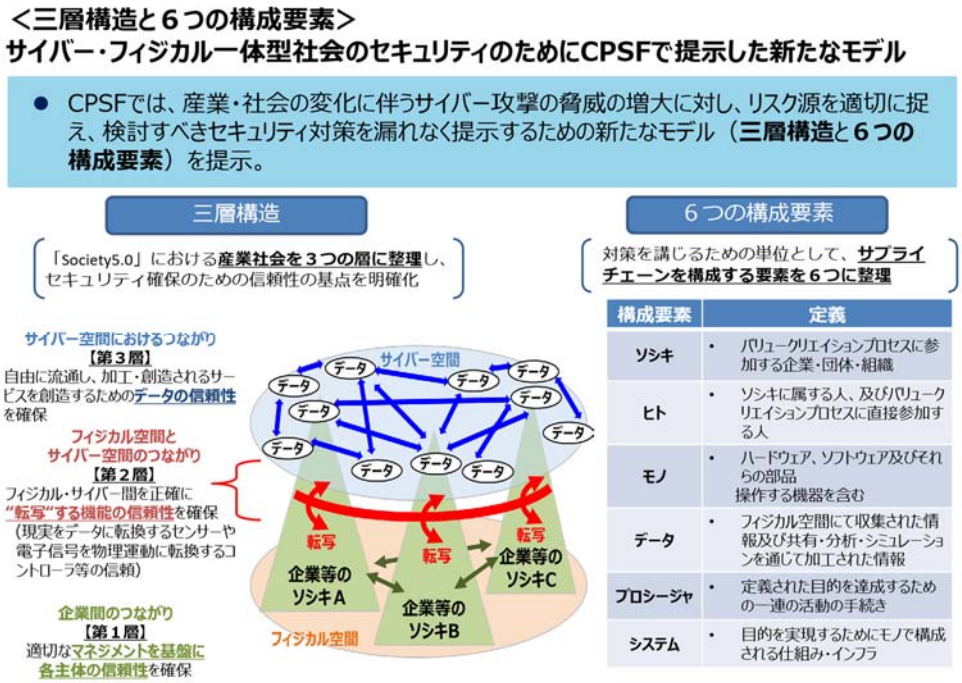
■サイバーセキュリティ政策の方向性

一般的には、認知しやすい DDoS 攻撃や入口対策に目が向きがちだが、サプライチェーンの中で深く静かに行われる攻撃準備への対応は非常に難しい。経済産業省では、セキュリティ政策の方向性転換の必要性を感じ、2017 年に新たな方向性を打ち出した。

まず、重要インフラについては BCP との連動、情報共有体制の強化、サプライチェーンに関しては産業ごとの対策強化、中小企業に寄り添い、サプライチェーンの中で生き残っていくため施策への転換を図る等、産業政策と連動した施策を展開する。さらにこれら施策の国際ハーモナイゼーションを確保するため、日本から積極的に提案を行う。また、実効性を持たせるため、セキュリティビジネスのエコシステム構築を支援するとともに、経営者の意識喚起や人材育成といった基盤整備を進める、という方針のもと取り組むこととした。これらの一連の施策の骨格となるものが、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）である。

■サイバー・フィジカル・セキュリティ対策フレームワーク

これまでは、プレイヤー各自が対策を行っていることが前提となっていたが、工場内に IoT が導入され、様々なところから上がってくるデータを利用する状況では、主体間の取組みだけでは対策が難しい。そのため、信頼のアンカーポイントを各所に入れ、それぞれのポイントでリスクや対策を確認する仕組み＝CPSF を考えた。CPSF では、産業社会を 3 つの層に捉え、各層を構成する要素を 6 つに整理している。



企業間のつながりである第 1 層は従来から考えられていた部分で、ここでの信頼のアンカーポイント（各主体のマネジメント）に対して、ISMS 等は重要な役割を果たしている。これに加え、Society5.0 においては第 2、第 3 層への対応も考える必要がある。第 2 層はフィジカル空間とサイバー空間がつながる部分（物理的な情報を電子データに転換する層）で、ここでの信頼のアンカーポイントは情報の転換機能（IoT 機器）となる。そして、転換されたデータの流通によりつながる第 3 層では、様々なプレイヤーによって加工・流通されるデータを利用するため、データそのものの信頼性を確保する必要がある。第 2 層、第 3 層では関わるプレイヤーも複雑化するため、マルチステークホルダーによる規律遵守が不可欠である。

さらに、信頼の基点がそれぞれ異なる各層でリスクベースアプローチを検討する際の単位として、サプライチェーンの構成要素を 6 つ（ソシキ、ヒト、モノ、データ、プロシージャ、システム）に整理し、各層で何を守るか、どのようなインシデントがあるか、リスク源は何か、どのように対策を行うかをまとめたものが CPSF である。策定にあたっては、英語版も含め 2 回のパブリックコメントを実施し国内外からの意見も反映させており、海外から参照したいという声もいただいている。

CPSF は標準的な内容であるため、現在、ビル、電力、防衛産業、自動車、スマートホームの分野ごとに特性を加味したガイドラインに落とし込む作業を行っている。また分野横断的な課題に対しては別に検討の場を設けている。業界別の検討では、特にビルは典型的なマルチステークホルダーで、誰が総合的にリスク対策を行うかが不明確であったため、先行して検討を行い 2019 年 6 月に第 1 版を公開している。

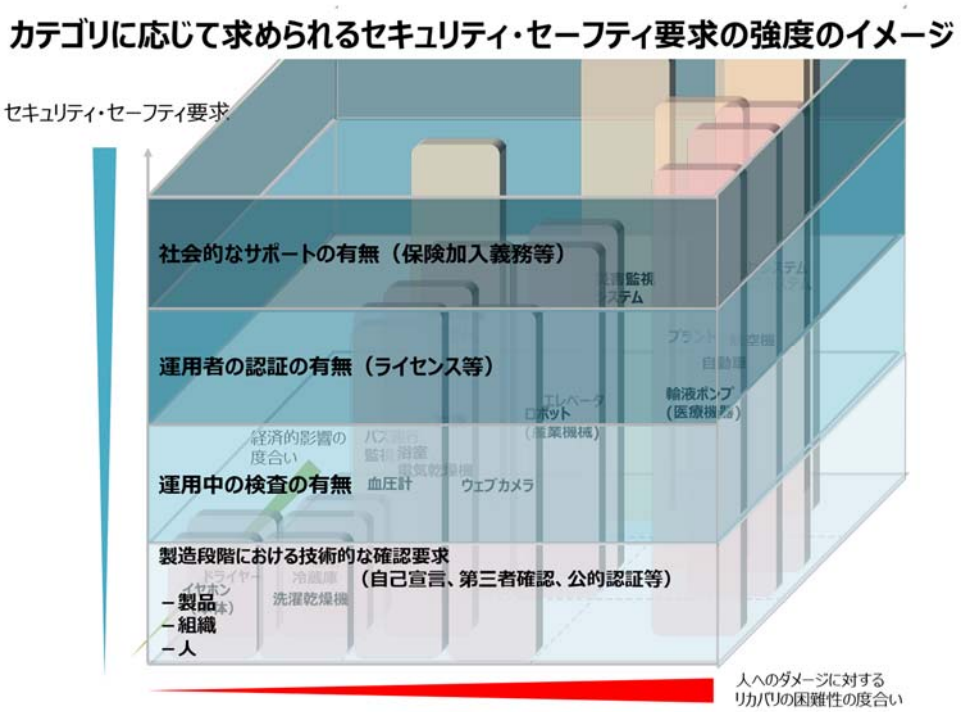
■分野横断的課題への対応

分野横断的課題検討の場として、現在、第 3 層のデータ信頼性確保を検討する「第 3 層タスクフォース（TF）」、オープンソースソフトウェア（OSS）の安全活用を考える「ソフトウェア TF」、第 2 層の機器の信頼性確保の要件を検討する「第 2 層 TF」が立ち上がっている。

第 3 層 TF：データセットごとのセキュリティ要件、データの信頼性確認手法を明確にし、データシェア促進につなげる。現在は、「データマネジメント」の定義を検討している。

ソフトウェア TF：非機能要求への対応が把握できない状況におけるソフトウェア管理手法や脆弱性対応の在り方を検討。まずは、OSS 活用のベストプラクティスを作り知見を共有することでソフトウェアマネジメントの最低限のレベル確保を図ろうとしている。

第 2 層 TF：EU では現在 IoT の認証が検討されており、米国では NIST がテクニカルリファレンスを提供し自主的な取り組みを促している。これらの動きと平仄を合わせる形で、日本は包括的フレームワークを検討している。具体的にはリカバリの困難性の度合いと経済的影響の度合いの二軸で整理し、それぞれに必要とされるセキュリティ・セーフティ要件を検討している。



これらの取り組みを、主体の責任・マネジメントといった信頼の基点の状況を ISMS、セキュリティ監査等により可視化する普遍的な取り組みの上に積み上げていくことで、新たな社会に対応していくことが必要と考えているが、Society5.0に向けたビジネスを加速させる上でさらに必要と思われるものがあれば、ぜひ経済産業省に要求していただきたい。