

[デジタルエコノミー時代のサイバーセキュリティ・デジタルトランスフォーメーション促進の基盤確立に向けて]

③ サプライチェーンサイバーセキュリティの強化に向けて —サイバー・フィジカル・セキュリティ対策フレームワークの策定—



奥家敏和 | 経済産業省商務情報政策局 サイバーセキュリティ課

「Society 5.0」の実現に向けて

IoT (Internet of Things)、人工知能 (AI) の利活用が進む中、世界ではドイツの「インダストリー 4.0」等、ものづくり分野で IT を最大限に活用し、第 4 次産業革命とも呼ばれる産業構造の変化を先導していく取組が官民協力の下で進展している。日本においても、2016 年 1 月 22 日に閣議決定された「第 5 期科学技術基本計画」^{☆1}にて、サイバー空間とフィジカル空間を高度に融合させることで、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society 5.0」を提唱している。

「Society 5.0」の推進によって、個別に機能するモノのシステム化と異分野間のシステム連携・協調の取組をものづくり分野だけでなくさまざまな分野に広げ、経済成長や健康長寿社会の形成、さらには社会変革につなげていくことが期待されている。IoT ですべての人とモノがつながり、さまざまな知識や情報が共有され新たな価値が生まれる社会、AI の分析により必要なモノやサービスが必要なときに必要なだけ提供される社会を目指していく一方で、急激に拡大するサイバー空間のセキュリティ確保がこれまで以上に重要となることは言うまでもない。

サイバーセキュリティを巡る状況の変化

サイバー攻撃の脅威の増大

IoT や AI の利活用が進む中で、サイバーセキュリティが直面する課題も増えている。具体的には、ネットワークにさまざまなモノがつながることで、サイバー攻撃の起点が増加するとともに、モノ・サービス等のやりとりをするサプライチェーンのつながりも複雑になるため、インシデントが発生した際の影響範囲も拡大する。また、サイバー空間とフィジカル空間の融合が進展することで、サイバー攻撃がフィジカル空間まで到達する危険性も増大する。さらには、IoT から得られる大量のデータの信頼性の担保や、流通・連携を支えるためのデータ管理も重要な課題である (図-1)。

防御側の視点では守るべき範囲が拡大する一方、セキュリティが弱いポイントを 1 か所見つけるだけでネットワーク内への侵入が可能というサイバー攻撃の特徴を踏まえれば、攻撃者の視点で考えると今まで以上に侵入が容易になりつつある状況といえる。このような状況においては、各企業のセキュリティ対策だけでサイバーセキュリティを確保していくことには限界がある。セキュリティ・バイ・デザインの観点を踏まえた各製品・サービス等の企画・設計段階からのサイバーセキュリティ対策に加えて、関連企業、取引先等サプライチェーン全体として、サイバー攻撃を受けた場合のビジネス活動の継続や復

^{☆1} <http://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf>

旧まで考慮に入れたセキュリティ対策に取り組むマルチステークホルダによるアプローチや、個々の主体を厳格に管理することが難しいデータ流通のセキュリティ対策も含めて、サイバーセキュリティ確保に取り組む必要がある。

高度化するサイバー攻撃

サイバー攻撃の脅威は、日本で認識されている以上に、海外では深刻な状況になっている。現在どのような水準に達しているのか、海外事例を中心に紹介する。

サプライチェーンを通じた攻撃

2017年5月に発生した WannaCry は、日本を含む世界150カ国以上で感染する事態となり、国内でも大きく報じられたことは記憶に新しい。業務システムなどいわゆるITシステムだけでなく、製造設備にも感染した結果、生産停止に陥るなど、企業活動にとって重大な影響を与えた事例もあった。2018年に入っても、台湾の半導体製造企業において WannaCry 亜種の感染に伴う生産停止により190億円の損害が発生した事例が報告されている。

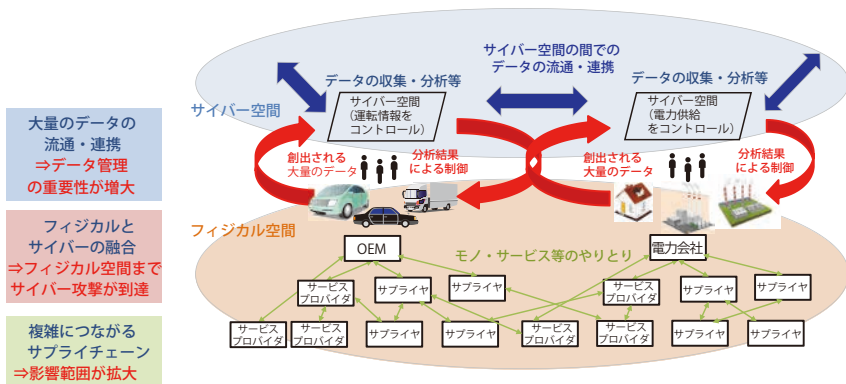
WannaCry の事例で注目すべき点は、サプライチェーンを経由した感染が発生したことである。データの利活用等、企業間でデータをシームレスにやりとりすることを通じてマルウェアに感染するリスクが高まっているが、日本国内でも、取引先の海外企業との画像データの交換を通じて国内事務所に感染が広がった事例が報告されている。子会社等の信頼

している企業間、もしくは内部システム間のデータ交換であっても、不審な振舞いを検知する仕組みを導入しておくなどの対策が必要になってきている。

電力システムへの攻撃

サイバー攻撃のレベルの高度化を示す事例として、ウクライナで2015年と2016年に発生した電力システムに対するサイバー攻撃を紹介する。特に、2016年の攻撃で使用された CrashOverRide というマルウェアは、検体の分析から制御系システムを対象とし、ウクライナの電力システムで利用されているプロトコルにも対応していたといわれている。一般的に、制御系システムは独自のソフトウェアやプロトコルを使っているため安全性が高いと考えられていたが、本事例ではサイバー攻撃のみによって停電という実害が引き起こされたと見られている。CrashOverRide はモジュールの追加により、電力システム以外の他の産業システムの独自プロトコルへの対応も可能なことから、制御系システム全般を対象として設計されていたことは明らかで、産業システムに対する脅威が現実のリスクとなった事例であるともいわれている。

米国の国家サイバーセキュリティ通信統合センター（NCCIC）が公表している「NCC/ICS-CERT Year in Review FY2016」^{☆2}では、重要インフラへのサイバー攻撃のうち、約1割の攻撃が制御系システムにまで到達したと報告されている。今後さらにこの割合は増えていく恐れがある。



■ 図-1 「Society 5.0」におけるモノ・データ等のつながりのイメージ

国内の動向

このようにサイバー攻撃が社会に与える影響が現実の脅威として顕在化しつつある中で、日本企業は欧米に比べてサプライチェーン

^{☆2} https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf

への対応が大幅に遅れているという状況が（独）情報処理推進機構が行った「企業のCISOやCSIRTに関する実態調査2017」^{☆3}により明らかになっている（図-2）。委託先のセキュリティ対策状況を把握している日本企業の割合は、米国の半分以下、欧州の3分の2以下、同じく調達先の状況把握についても欧米の6割以下となっている。自社の状況把握は欧米に比して大きな差がないため、余計に委託先、調達先への対応の遅れが際立っている。

海外の動向

海外に目を向けると、欧米を中心にサプライチェーンのサイバーセキュリティに対する要求が高まっている。特に、IoTやICS（産業用制御システム）をサイバー攻撃から防御するためには、サプライチェーン管理からアプローチする必要性が広く認識されるようになっている。

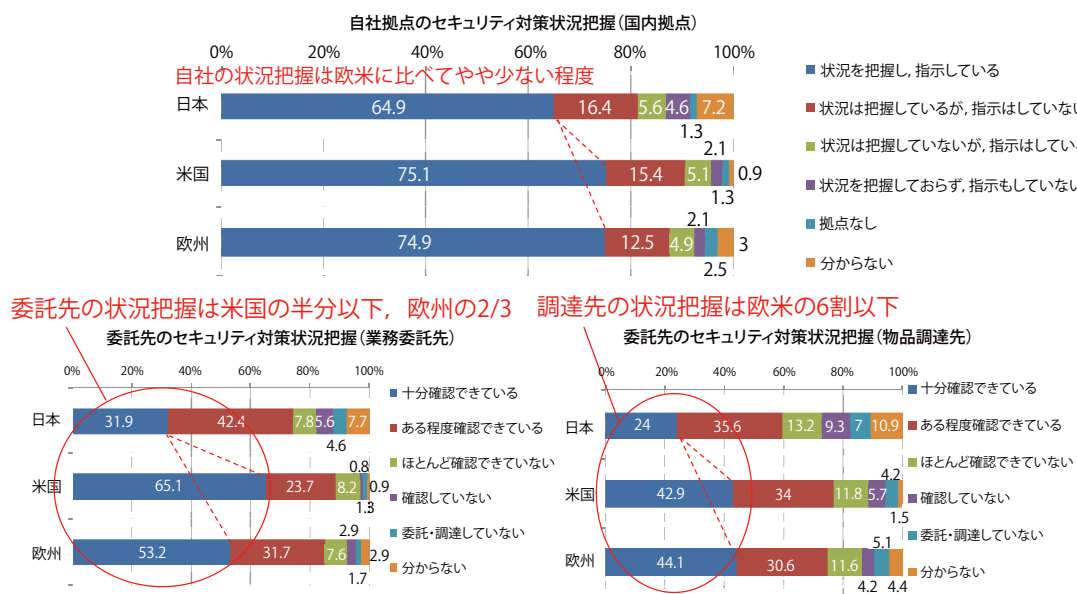
米国では、米国国立標準技術研究所（NIST）がサイバーセキュリティ対策の全体像を示したフレームワークを2014年2月に策定しているが、2018年

4月の改訂により、サプライチェーンのリスク管理を行うことが追記された。具体的には、サプライチェーン全体でセキュリティ対策を実施することや、必要に応じて監査を行うことを新たに要求している。また、2017年末には防衛調達に参加する企業であって機密性の高い情報を共有する企業に対して、SP800-171に規定されたサイバーセキュリティ対策の遵守が義務化された。

欧州では、2017年9月に、ネットワークにつながる機器の認証フレームワークの導入検討が発表され、現在も議論が行われている。また、2018年5月には、エネルギー等の重要インフラ事業者に対してサイバーセキュリティ対策を義務化する指令（NIS Directive）と、欧州の顧客データを扱う企業に対してデータ保護に新たな義務を課すEU一般データ保護規則（GDPR）がそれぞれ施行された。

米国は安全保障の観点から、欧州はプライバシー保護の観点から、サイバーセキュリティに関する政策を推進しているが、このような取組によってセキュリティ要件を満たすことができない事業者、製品、サービスがグローバルサプライチェーンからはじき出さ

☆3 <https://www.ipa.go.jp/files/000058850.pdf>



* 日本・米国・欧州（英・独・仏）の従業員数300人以上の企業のCISO、情報システム／情報セキュリティ責任者／担当者等にアンケートを実施（2016年10月～11月）
* 回収は日本755件、米国527件、欧州526件

■図-2 取引先へのサイバーセキュリティ対策の遅れ

れる恐れが出てきている。サイバーセキュリティの問題は、日本企業がグローバルサプライチェーンに引き続き参加し、ビジネスを継続することができるかを左右する課題になりつつあるといえる。

経済産業省における取組

このようなサイバーセキュリティを巡る状況に対し、経済産業省では、産業におけるサイバーセキュリティ政策を4つの柱（図-3）で捉え、政策の方向性を示すべく、2017年12月に産業サイバーセキュリティ研究会を立ち上げた。さらにその下に3つのワーキンググループ（WG）を設け、「制度・技術・標準化」「経営・人材・国際」「サイバーセキュリティビジネス化」のテーマごとにそれぞれ議論を行っている。各WGの議論を踏まえ、2018年5月に開催した第2回研究会では、「サプライチェーンサイバーセキュリティ強化」「サイバーセキュリティ経営強化」「サイバーセキュリティ人材育成・活躍促進」「セキュリティビジネスエコシステム創造」の4つのパッケージからなるアクションプラン^{☆4}を公表した。特に、サプライチェーンのサイバーセキュリティ強化に向けては、前述した「制度・技術・標準化」WGを中心に、産業に求められるセキュリティ対策の全体像を整理し、産業界が活用できる「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「フレームワーク」とする）の策定を進めている。

サイバー・フィジカル・セキュリティ対策フレームワーク

フレームワークの目的

あらゆるものがつながる「Society 5.0」が実現された社会では、産業構造が変化し、製品・サービスを生み出す工程（サプライチェーン）も従来の固定

的・安定的なものとは異なる、多様なつながりによる非定型の付加価値創造活動へと変化していくことが想定される。フレームワークは、このような「Society 5.0」型サプライチェーンを従来のサプライチェーンと区別するため、「価値創造過程（バリュークリエーションプロセス）」と定義し、「Society 5.0」によって拡張されたサプライチェーンの概念に求められるセキュリティ対策の指針を示すものである。

フレームワークの考え方

バリュークリエーションプロセスでは、従来のサプライチェーンの信頼できる企業間のつながりによる付加価値創造活動が大きく拡張される。すなわち、フィジカル空間の情報はIoTによってデジタル化され、データとしてサイバー空間に取り込まれ、取り込まれたデータはサイバー空間で自由に流通する。その結果、多様なデータの利活用から創出される新たなデータや、それらのデータがIoTによってフィジカル空間にフィードバックされることで創出される新たな製品やサービスなどにより付加価値が創出される。フレームワークの検討にあたっては、このような新たな付加価値を創造する一連の活動を視野に入れた整理が必要である。

そのため、従来のサプライチェーンの活動範囲から拡張された、付加価値を創造する活動のセキュリティ上のリスクを的確に洗い出し、対処方針を示す

1. 産業政策と連動した政策展開	① 重要インフラの対策強化 情報共有体制強化 等
	② IoTの進展を踏まえたサプライチェーンごとの対策強化 (Industry by industry) - 防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進
	③ 中小企業のサイバーセキュリティ対策強化
2. 国際ハーモナイゼーション	① 日米欧間での相互承認の仕組みの構築
	② 民間主体の産業活動をゆがめる独自ルールの広がり阻止
3. サイバーセキュリティビジネスの創出支援	① 産業サイバーセキュリティシステムを海外に展開
	② サービス認定創設、政府調達などの活用
4. 基盤の整備	① 経営者の意識喚起
	② 多様なサイバーセキュリティ人材の育成（ICSCoE等）
	③ サイバーセキュリティへの過少投資解決策の検討

■図-3 サイバーセキュリティ対策の方向性

^{☆4} http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/002_03_00.pdf

ために、フレームワークでは付加価値の創造が営まれる社会を3つの層に分けた構造として整理している。具体的には、「企業間のつながり」を捉える第1層、「フィジカル空間とサイバー空間のつながり」を捉える第2層、そして「サイバー空間におけるつながり」を捉える第3層である（図-4）。

このように捉えることで、第1層では適切なマネジメントを基盤とした各主体の信頼、第2層ではフィジカル空間の情報をサイバー空間に正確に取り込む、あるいはサイバー空間のデータをフィジカル空間に正確にフィードバックするIoT機器のフィジカル・サイバー間の“転写”機能の信頼、そして第3層ではサイバー空間上を自由に流通するデータそのものの信頼という、バリュークリエーションプロセスにおいて確保されなければならない機能・役割に応じた整理が可能となる。

この3層構造に基づいて、各層で守るべきもの、セキュリティリスクの洗い出しを行い、「組織」「ヒト」「モノ」「データ」「プロセス」「システム」という6つの構成要素ごとに、どのようなセキュリティ対策を行うべきか方針を整理して示している（図-5、6）。

サイバー・フィジカル・セキュリティの確保

フレームワークを活用して、どのようにバリュークリエーションプロセス全体のセキュリティ確保を実現するか。そのためには、信頼のチェーンの構築と維持が必要となる。

信頼のチェーンとは、バリュークリエーションプロセス内の構成要素のセキュリティ確保（信頼の創出）と、その確認（信頼の証明）とを繰り返すことで連鎖的に構築される信頼関係のつながりである。「信頼の創出」には、セキュリティ要件を満たすモノ・

データ等の生成に加え、それらがセキュリティ要件を満たす形で生成されていることを確認できることが、「信頼の証明」には、構成要素に対して創出された信頼を管理し、その信頼を対外的に確認できる仕組みがそれぞれ求められる。

信頼のチェーンを構築し、そのつながりをたどることでトレーサビリティが確保できる。その上で、外部からの攻撃等の検知・防御やレジリエンス強化などの対策を講じると、構築した信頼のチェーンが壊されないよう維持していく必要がある。

フレームワーク策定に向けて

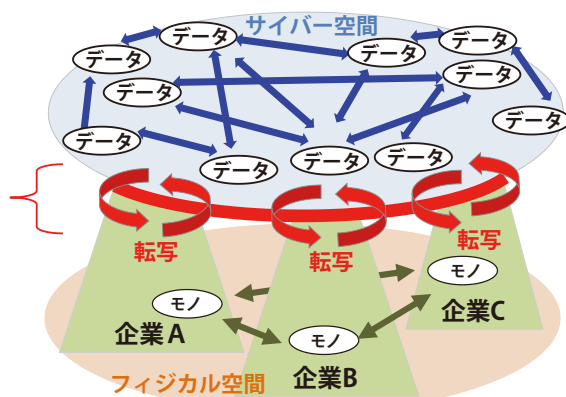
このような考え方に基づいてフレームワーク案を作成し、国内外から広く意見を求めるべく、2018年4月末から1カ月間パブリックコメントを実施した^{☆5}。その結果、国内23、海外10の組織・個人から300件を超える意見提出があり、これらの意見を踏まえたフレームワークの考え方の明確化や対処方針の具体化、既存の国際規格との対応関係の整理等を進めている。より分かりやすい記載となるよう、構成変更を含めた修正を行うことから、再度のパブリックコメント実施を検討している。

また、フレームワークの検討と並行して産業分野別のセキュリティ水準の検討を進めている。フレームワークは「Society 5.0」における共通的なセキュ

☆5 <http://www.meti.go.jp/press/2018/05/20180502003/20180502003.html>

- サイバー空間におけるつながり**
【第3層】
- ・自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保
- フィジカル空間とサイバー空間のつながり**
【第2層】
- ・フィジカル・サイバー間を正確に“転写”する機能の信頼を確保
(現実をデータに転換するセンサや電子信号を物理運動に転換するコントローラ等の信頼)
- 企業間のつながり（従来型サプライチェーン）**
【第1層】
- ・適切なマネジメントを基盤に各主体の信頼を確保

■図-4 3層構造アプローチ



リティ対策の枠組みを示すものの、それぞれの業界や企業によって、守るべき重要な資産、人的・資金的リソース、許容できるリスク等はさまざまであり、実際に優先すべきセキュリティ対策も異なるためである。具体的には、電力分野やスマートホーム分野等でそれぞれ検討を開始しており、特に、ビル分野では2018年9月に「ビル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(β版)」^{☆6}をとりまとめている。今後、分野別の検討を進めた上で、横断的課題を相互にフィードバックし、各産業分野に共通する対策を洗い出すなどの取組も進めていく。

「Society 5.0」における信頼の確保に向けて

本稿では、「Society 5.0」が実現される社会で求められるセキュリティ対策の考え方や、具体的な対策指針を整理した、「サイバー・フィジカル・セキュリティ対策フレームワーク」の策定に向けた取

組を紹介した。サイバー攻撃が社会に与える影響が深刻になる中で、本稿がサプライチェーン全体でのセキュリティ対策の必要性を認識する機会となれば幸いである。また、各業界や各企業においても、それぞれの実態に則した脅威・リスクシナリオの想定、リスクアセスメントや具体的なセキュリティ対策の検討などにフレームワークを活用いただきたい。

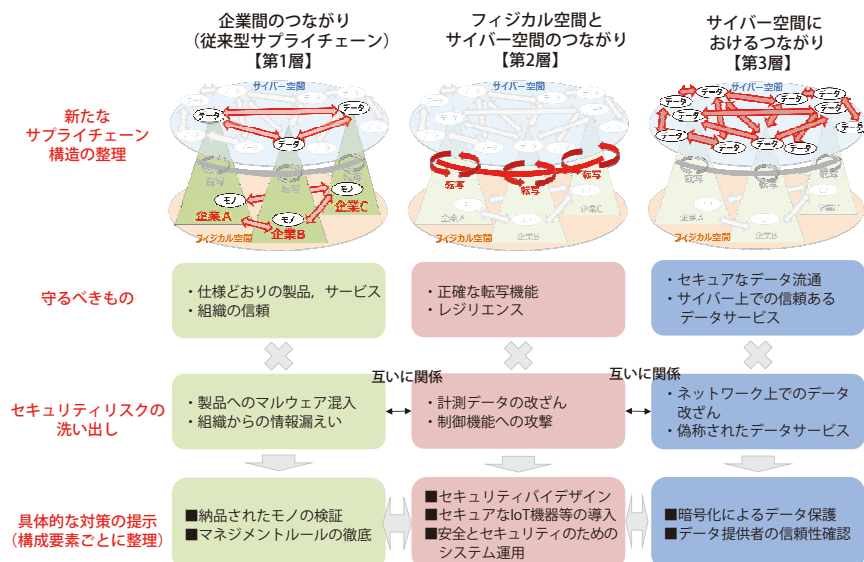
フレームワークの策定後も、先に説明した「信頼の創出」や「信頼の証明」の実現に必要な制度面の検討や、サプライチェーンサイバーセキュリティにかかわる研究開発の推進、日本のセキュリティニーズに応じた日本発のサイバーセキュリティ製品の有効性等を検証するための検証基盤の構築など、フレームワークを中心に、「Society 5.0」におけるサイバー・フィジカル・セキュリティ確保の実現に向けた取組を進めていく。

(2018年9月17日受付)

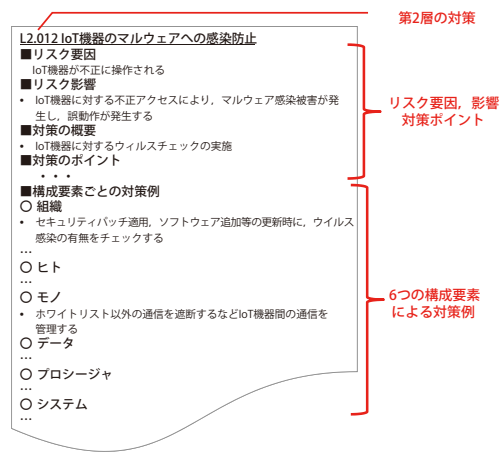
奥家敏和

1995年通商産業省(当時)入省。JETRO ニューヨーク、2013年資源エネルギー庁官房総合政策課、2015年貿易経済協力局貿易管理部安全保障貿易管理課長、2016年安全保障貿易管理政策課長を経て、2017年より商務情報政策局サイバーセキュリティ課長。

^{☆6} http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20180903_report.html



■図-5 各層におけるセキュリティ対策の概要



■図-6 対策指針の記載例