特集
Special Feature

［DX（デジタル・トランスフォーメーション）時代のサプライチェーン・セキュリティ］

2 サイバー・フィジカル・セキュリティ・フレームワークを活用したサプライチェーン・セキュリティの確保

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

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）の策定

我が国では，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により，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」の実現を提唱している．また，経済産業省では，「Society 5.0」の実現へ向けてさまざまなデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し，その実現に向けた取り組みを推進している．

あらゆるものがつながる「Society 5.0」「Connected Industries」では，企業間・産業間のネットワーク化が進展して新たなつながりが生まれる中で，付加価値を創造するための一連の活動であるサプライチェーンの形態も，これまで取引することのなかった新たな相手を巻き込んだ柔軟かつ動的な構成へと変化する．また，サイバー空間とフィジカル空間が相互に作用しあう中での新たな付加価値の創造も期待される．

高度にネットワーク化され，動的に構成されるサプライチェーンにさまざまな主体が参加するような状況においては，一企業が取り組む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．このため，それぞれの企業がセキュリティ・バイ・デザイン等の観点を踏まえて，企画・設計段階から製品やサービスのサイバーセキュリティ対策を実施することに加え，ビジネス活動のレジリエンスまで考慮に入れた上で，関連企業，取引先等を含めたサプライチェーン全体として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，データ流通におけるセキュリティも含めて，サイバーセキュリティ確保に取り組む必要がある．そのため，経済産業省では，「産業サイバーセキュリティ研究会ワーキンググループ1（制度・技術・標準化）」を中心として，新たな産業社会において付加価値を創造する活動が直面する新たなリスクに対応していくためのセキュリティ対策の指針を「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，「CPSF」）として取りまとめ，2019年4月18日に初版を公表した．

CPSFは，産業界全体を対象としたサイバーセキュリティ対策を考えるためのモデル的枠組みである．一方，各産業分野で守るべき資産やセキュリティ対策に割けるリソース等が異なることから，WG1の下に産業分野別SWGを設置し，CPSFをベースに各産業分野におけるセキュリティ対策の検討を進めている．その上で，CPSFをベースに対策を進めるにあたって，サイバー空間とフィジカル空間のつながりにおける信頼性の確保やソフトウェア管理など，さらに詳細な検討が必要とされる分野横断的課題を検討するために，3つのタスクフォース（TF）を設置し，議論を進めている．

本稿では，CPSFの基本的な考え方およびCPSFの社会実装に向けた取り組みの1つとして，分野横断的課題の1つであるIoT機器・システムにもとめられるセキュリティ・セーフティ対策についてま

© 2021 Information Processing Society of Japan

とめたIoTセキュリティ・セーフティ・フレームワークについて紹介する．

サイバー・フィジカル・セキュリティ対策フレームワークの概要

三層構造と6つの構成要素

CPSFでは，新たな社会における付加価値を創造する一連の活動のセキュリティ上のリスク源を的確に洗い出し，対処方針を示すために，図-1に示すように，産業社会を「企業間のつながり」「フィジカル空間とサイバー空間のつながり」および「サイバー空間におけるつながり」という3つの切り口で捉えている．セキュリティ確保に求める信頼性の基点をこの3つの切り口で捉えるモデルを活用することで，新たな環境におけるリスクを整理することができる．

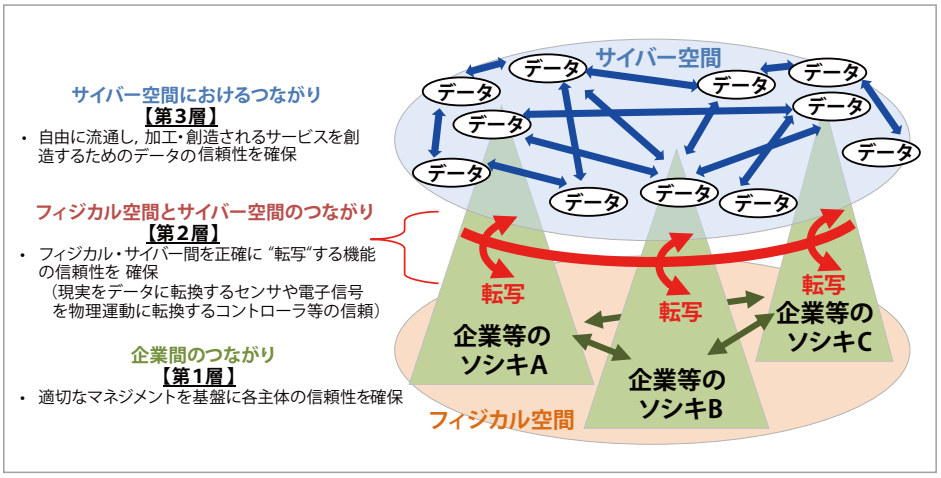
第一層：企業間のつながり

まず，「企業間のつながり」では，企業・組織のマネジメントの信頼性の確保が求められる．サプライチェーンのセキュリティを実現する上で従来から採用されてきた考え方であり，セキュリティ対応をしっかりと行った企業・組織間で行われる定型的・直線的な取引であれば，その活動全体のセキュリティが確保されるという考え方が前提となっている．しかしながら，サイバー空間とフィジカル空間が一体化した産業社会においては，企業・組織のマネジメントの信頼性を確認するだけでは，そのプロセス全体の信頼性を確保することは難しい．そのため，以下で説明するように，企業・組織のマネジメントとは異なる信頼性の基点を設定し，その信頼性を確認することが必要になる．

第二層：フィジカル空間とサイバー空間のつながり

次に，「フィジカル空間とサイバー空間のつながり」では，フィジカル空間とサイバー空間の境界において，要求される情報に応じて適切な正確さでフィジカル空間とサイバー空間の間で情報を変換する，いわば「転写」機能の正確性が信頼性の基点となる．「Society 5.0」では，フィジカル空間からサイバー空間に「転写」されたデータがさまざまな主体間で自由に流通するとともに，サイバー空間でさまざまな主体が加工・編集したデータがフィジカル空間に展開することで付加価値を創出することとなる．その際，両空間の境界において転換される情報の変換は高い正確性を求められ，「転写」の正確性が確保されなければ，柔軟かつ動的なサプライチェーンの信頼性を確保されることはない．

実際のサイバー空間とフィジカル空間の境界は，センサ，アクチュエータ，コントローラといった，いわゆるIoT機器・システムによって構成されるが，この境界におけるフィジカル空間とサイバー空間の間を「転写」する機能は，企業・組織のマネジメントの信頼性の確認だけでは確保することはできない．機器・システムの供給者や保守事業者などを含めて，その機能を構成するモノの信頼性や構築・保守の信頼性を確保する取り組みが必要であり，ライフサイクル全体を



■図-1　三層構造モデルと各層における信頼性

© 2021 Information Processing Society of Japan

視野に入れた信頼性の確認などがなされて初めて信頼性が確保されるといえる．

第三層：サイバー空間におけるつながり

最後に，「サイバー空間におけるつながり」では，サイバー空間で流通するデータそのものが信頼性の基点となる．サイバー空間では，多様なデータが生成・編集・加工され，さまざまな主体の間で自由に流通するすることで，柔軟で動的なサプライチェーンが形成されることとなり，それこそがサイバー空間で付加価値を創造する基礎となる．「Society 5.0」「Connected Industries」では，マネジメントの信頼性が確認された企業・組織だけではなく，さまざまな主体がこれらの活動に関与する可能性があることや，また，主体が判明しないデータを活用しなければならないことにも留意しなければならない．そのため，目的どおりの価値を創造するためには，プロセスに関与するデータそのものの信頼性の確保が不可欠となる．

このように，サイバー空間とフィジカル空間が一体化した社会における付加価値の創造活動においては，3つの視点から信頼性を確保するセキュリティの取り組みが必要であり，これらを「層」として信頼性の基点と捉えることで，発生し得るインシデント，そのリスク源を明らかにし，対策の方向を示すことが可能となる．

リスク源の洗い出しと対応方針の整理

三層構造モデルに基づいて，各層において守らなければならない機能・役割の整理が可能となる．CPSF では，表 -1 に示すように各層の特性，機能・役割と想定される分析対象の具体的イメージをはじめとして，新たなリスク源を洗い出す際に考慮すべき観点をまとめており，リスクアセスメントにおける分析対象の明確化に活用することができる．

セキュリティ対策の概要

CPSF では，図 -2 に示すように，各層における機能，セキュリティインシデント，リスク源，対策要件を整理している．具体的には，CPSF の添付 B で各層の機能，想定されるセキュリティインシデント，セキュリティインシデントを引き起こし得るリスク源と，リスク源に対するセキュリティ対策要件との対応関係を示している．また，添付 C では，実際にセキュリティ対策を講じる場合の対策の範囲や，対策を導入・運用する場合の相対的コスト等を考慮したレベル別のセキュリティ対策例を示している．これらを活用することで，企業・組織等のセキュリティ対策の担当者は，対象となる企業・組織等の

■表 -1
三層構造に基づく分析対象および具体的イメージ

階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンス・マネジメント	・各組織のセキュリティマネジメント 【信頼性の基点】組織・マネジメント	・組織で管理されるモノ・システム 等 ・組織内で流通するデータ 等	・社員，従業員 ・企業のIT資産 等
第2層	フィジカル空間とサイバー空間のつながり拡大	・フィジカル空間とサイバー空間との間のデータのやりとり 【信頼性の基点】ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	・データを転写するモノ・システム ・転写されるデータ 等	・センサ ・アクチュエータ ・3Dプリンタ ・監視カメラ 等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	・データの送受信，加工・分析，保管 【信頼性の基点】データ	・データを送受信／加工・分析／保管するモノ・システム ・組織を超えて流通するデータ等	・サーバ ・ルータ ・スマートメータ ・オープンデータ 等

© 2021 Information Processing Society of Japan

システムや動的に重要度が変化する守るべき資産の重要度，リスクアセスメントの結果に応じた適切なセキュリティ対策を検討することができる．

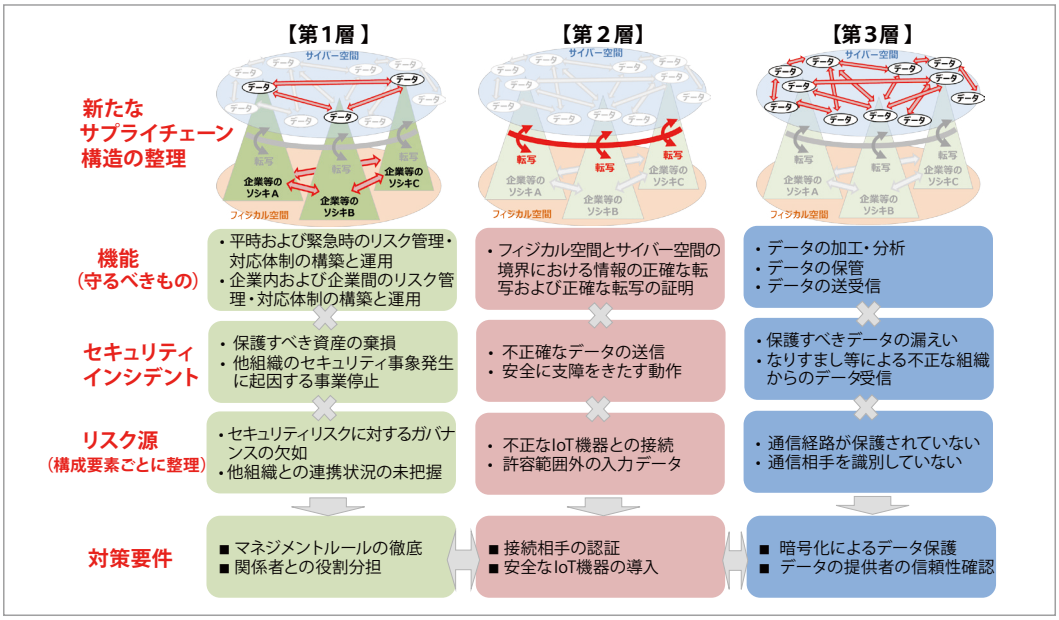
CPSF のさらなる社会実装に向けて

経済産業省サイバーセキュリティ課では，CPSF の産業界への具体的な実装を目指して，産業構造や商習慣などの観点を踏まえて，各産業分野で求められる具体的なセキュリティ対策の検討を推進している（図 -3）．特に，さらに，IoT 機器・システムの信頼性（第 2 層），データマネジメント（第 3 層），ソフトウェアの管理手法といった産業横断的な対策が求められる課題については，タスクフォースを立ち上げて別途検討を進めている．

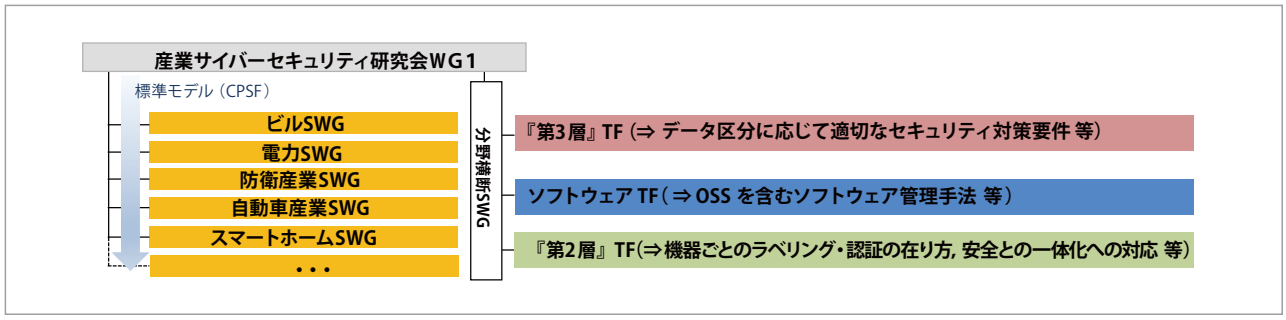
IoT セキュリティ・セーフティ・フレームワークの策定

先述のとおり，「Society 5.0」においては，フィジカル空間とサイバー空間の境界における転写機能の正確性を確保することが特に重要となる．フィジカル空間とサイバー空間をつなぐ機器・システム，すなわち IoT 機器・システムのセキュリティの確保が重要になる．

IoT セキュリティガイドライン（平成 28 年 7 月 IoT 推進コンソーシアム，総務省，経産省）でも触れられているように，簡易な情報サービスの分野に使用される IoT 機器と，工場や社会インフラシス



■図 -2
各層におけるセキュリティ対策の概要



■図 -3　CPSF に基づくセキュリティ対策の具体化・実装の推進

© 2021 Information Processing Society of Japan

テム等の安全にかかわる分野で使用されるIoT機器では，求められるセキュリティレベル，セキュリティ対策の目的，優先度が異なる．今後，IoTの活用の拡大に伴い，それぞれの分野の特殊性・多様性を踏まえて，使用分野ごとに個別・具体的なIoT機器・システムに対して実際のセキュリティ対応が進んでいくことになると考えられる．その過程において，サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して，包括的に課題を捉える統一的な手法が欠如しているため，それぞれの分野や業界において別々の検討プロセスを経て，独自のセキュリティ・セーフティ対策等が設定されることが懸念される．それぞれの対応策に不整合が生じれば，社会として新たな仕組みを受容・管理していくためのコストが増大する恐れがある．そこで，IoTシステムの信頼性（第2層）に関する横断的課題議論するTFにおいては，『サイバー空間とフィジカル空間のつながり』における信頼性確保をテーマに議論を行い，IoTセキュリティ・セーフティ・フレームワークを策定した．

フレームワークの基本的考え方

サイバー空間とフィジカル空間をつなぐ新たな仕組みであるIoTにはさまざまな形態およびそれに伴うセキュリテ ィ上の課題があり，さらに，実際にインシデントが発生した場合の被害の態様もきわめて多様である． IoTを構成する機器・システムに対して一律のセキュリティ要求を設定した場合，仮にその要求が満たされていても，それでは多様なセキュリティ上の課題に十分に対応することは できない．

IoT機器・システムのセキュリティ対策を検討する際は，この多様性に対してどのようにアプローチするのかがポイントとなる．本フレームワークでは，サイバー空間とフィジカル空間をつなぐ新たな仕組みであるIoT機器・システムの“多様性”という論点にアプローチするための手段として，この仕組みを構成する機器・システムについて，リスクの捉え方とその対応にかかる基本的な考え方を集約した3つの軸を活用し，カテゴライズするとともに，適切な対策の内容を整理して比較・検討できるようにすることを提案している．

IoT機器・システムに潜むリスクの整理

前述のとおり，IoT機器･システムのセキュリティ上の課題は多様なものである．そこで，IoT機器・システムに潜むリスクに基づいてカテゴライズし，マッピングする2つの軸を設定することとした．

第1軸は，発生したインシデントの影響の回復困難性の度合いである．回復の困難性については，まず，人命が失われればそれが回復されることはない．また，インシデントの発生の結果，重度の身体障害が発生した場合，完全に回復できるとはいえないケースが少なくない．こうした，インシデントによる影響が回復できるものか否か，また，回復ができるものについては早期の回復ができるか否か，という判断軸を第1軸として設定した．

第2軸は，インシデントによる資産の毀損，経済活動や社会への影響等の事象を金銭的価値に換算した場合の大きさを基準としたものである．

2軸の整理を基に機器・システムをマッピングした例を図-4に示す．前述のとおり，IoT機器・システムのセキュリティ上の課題は多様であるため，それぞれの機器・システムにおける適切な対策も一様ではない．しかしながら，このカテゴリに基づいて検討を行うことで，一般に右上にカテゴライズされるものほどインシデントによる影響が大きい傾向があるため，より重厚な対策が必要であると考えられる一方，左下にカテゴライズされるものほど，軽微な対策で十分な可能性があると整理することが可能となる．

求められるセキュリティ・セーフティ要求の整理

第1軸と第2軸を活用し，フィジカル・サイバー間をつなぐ機器・システムについて，そのリスクを踏まえてカテゴライズした上で，本フレームワークでは，IoT機器・システムのセキュリティ対策を包

© 2021 Information Processing Society of Japan

括的に整理するために，求められるセキュリティ・セーフティ要求の観点という第３軸を設定する．

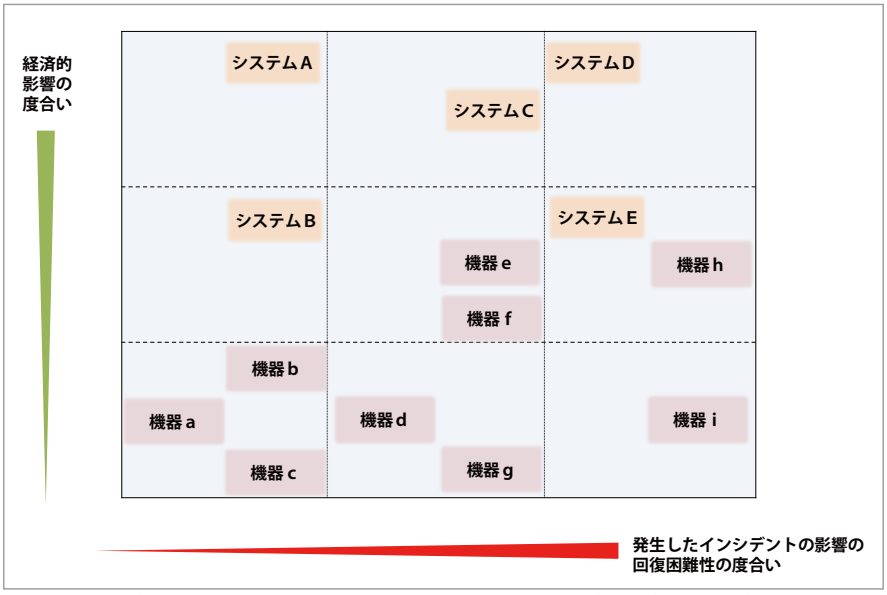
第３軸は，図 -5 のように第１軸と第２軸で形成される平面に直交する形で，いわば３次元を構成し，第１軸と第２軸によって整理されたそれぞれのカテゴリに求められるセキュリティ・セーフティ要求の観点を示す役割を果たすものである．

第３軸は，セキュリティ・セーフティを確保するための手法を以下の４つの観点から整理している．

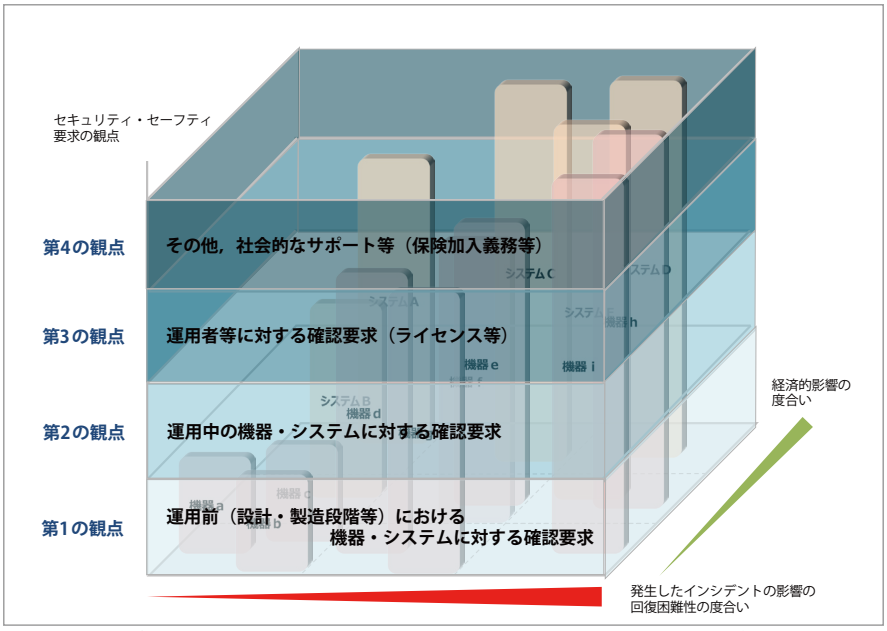
第１の観点は，運用前（設計・製造段階等）における機器・システムの確認要求である．IoT 機器が実際に利用に供される前の段階で，機器・システムそのものが必要なセキュリティ・セーフティ対策を講じられていること，または当該機器・システム等の生産者や供給者，検査者，場合によっては生産設備・工場等が必要な能力条件等を満たしていることなどを確認することを求めるものである．確認の方法に関しては，自己宣言や第三者認証などさまざまな形態があるが，求められる確認レベルの専門性や客観性を踏まえて設定されることとなる．

第２の観点は，運用中の機器・システムに対する確認要求である．運用中に発生する故障や，実施されるソフトウェアのアップデートやメンテナンスなどによって，想定外の問題が発生する可能性があることから，運用開始後に，ライフサイクルやサービス期間も考慮しながら機器・システムを確認することを求めるものである．この観点の確実な実施を求めていくためには各ステークホルダにおいて役割や責任分界点を明確化するなど，より社会的な仕組みを用意することが必要となる．

第３の観点は，機器・システムの運用・管理を行う者の能力に関する確認要求である．機器・システムの誤使用・誤操作などによって発生するインシデントの影響が，セキュリティ・セー



■図 -4　フィジカル・サイバー間をつなげる機器・システムのカテゴライズのイメージ



■図 -5　カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ

© 2021 Information Processing Society of Japan

フティ対策だけでは許容できる水準ではない場合には，機器・システムの運用・管理を行う者が当該機器・システムを適切に運用・管理するために必要な能力を持っていることを確認することを要求することになる．

第 4 の観点は，そのほか，社会的なサポート等の仕組みの要求である．インシデントが発生した場合の影響が非常に大きく，当該仕組み等の所有者が個々に賠償等の対処を実施することが容易ではないケースの場合には，あらかじめ保険加入を義務付けるなどの社会的なセーフティネットを講じることを求めるものである．

なお，第 3 軸における 4 つの観点は，それぞれが必ずしも完全に独立したものではない一方，必ずしもすべての観点での要求が求められるものではない．複数のステークホルダが関係するリスクへの対処は，複数の観点から行えることから，関係するステークホルダにおける負担について，各ステークホルダが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて，総合的に検討し，ステークホルダ間で合意する必要がある．したがって，機器・システムに対する直接的な対策は当然重要ではあるが，単独のステークホルダがすべての要求に対処する必要はなく，また，ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である．

フレームワークの活用の促進に向けて

今後，IoT を活用しようとする主体が本フレームワークを活用することにより，一定程度の整合性を確保しながらセキュリティ・セーフティ対策を検討することが可能となる．本フレームワークの活用がより一層促進されるため，ユースケースの整理を進めていく予定である．

（2020 年 12 月 22 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長官官房総合政策課，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 年より現職．

© 2021 Information Processing Society of Japan