Ⓡ 研究論文

サイバー・フィジカル・セキュリティ対策の実装と保証

Implementation and Assurance of The Cyber/Physical Security Framework

成田　和弘
Kazuhiro Narita

三菱 UFJ トラストシステム株式会社
Mitsubishi UFJ Trust Systems Co., Ltd.

概　要

「サイバー・フィジカル・セキュリティ対策フレームワーク」は、経済的発展と社会的課題の解決を実現する Society5.0 における「価値創造過程（バリュークリエイションプロセス）」のセキュリティを確保するために策定された。信頼性の基点を 3 つの層と 6 つの構成要素によって整理し、組織のマネジメントの信頼性にのみ基点を置くのではなく、“各構成要素について必要なセキュリティ要件が満たされていることを確認”できる「信頼の創出」と「信頼の証明」により「信頼のチェーンの構築と維持」を実現することを目指している。本稿では、この実装には、「バリュークリエイションプロセスの役割と責任の明確化」、「効率的なセキュリティ実装による対応コストの削減と対応速度の向上」が必要であり、その保証にあたっては、「調達者の要求が実装されていることの保証」、「サービスの機能安全の保証」と「変化対応が可能な保証の枠組み」による継続的な保証の実現が課題となることを指摘する。そしてその課題解決に資する方策として、「アグリゲート・コンピューティング・モデル」のアーキテクチャや、「開放系総合信頼性技術」等の品質保証技術の活用を提案する。監査人は、「信頼の創出」と「信頼の証明」、「信頼のチェーンの構築と維持」に関与して「バリュークリエイションプロセス」の信頼を実現するため、クラウドを活用した新しいアーキテクチャと、複雑化したシステムにおける品質保証技術を理解する必要がある。

キーワード：Society5.0、品質保証（QA）、機能安全、セキュリティ / セーフティ・バイ・デザイン、ソフトウェア・ライフサイクル、コモンクライテリア（CC）、開放系総合信頼性技術、アグリゲート・コンピューティング・モデル、NIST-SP1800、クラウド

1．はじめに

我が国は「Society5.0」を提唱し、経済的発展と社会的課題の解決の両立を目指している。その産業社会は、サイバー空間とフィジカル空間を跨いだ、これまでより柔軟で動的な新たな形のサプライチェーンで構成され、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。2019 年 4 月に策定された「サイバー・フィジカル・セキュリティ対策フレームワーク[1]（以下 CPSF）」では、このサプライチェーンを「バリュークリエイションプロセス」と呼び、その活動が直面する「サイバー攻撃の起点の拡大とその被害の影響の増大」という新たなリスクに対応し、信頼性を確保することを目指している。

本稿では、CPSF の考え方を概観した上で、その実装には、「バリュークリエイションプロセスの役割と責任の明確化」、「効率的なセキュリティ実装による対応コストの削減と対応速度の向上」が必要であり、その保証にあたっては、「調達者の要求が実装されていることの保証」、「サービスの機能安全の保証」、「変化対応が可能な保証の枠組み」が課題となることを指摘し、その課題解決に資する方策と、監査人がどのように「バリュークリエイションプロセス」の保証に関与すべきか

投稿受理日	2020 年 3 月 19 日
査読完了日	2020 年 4 月 27 日

について考察する。

2．関連研究

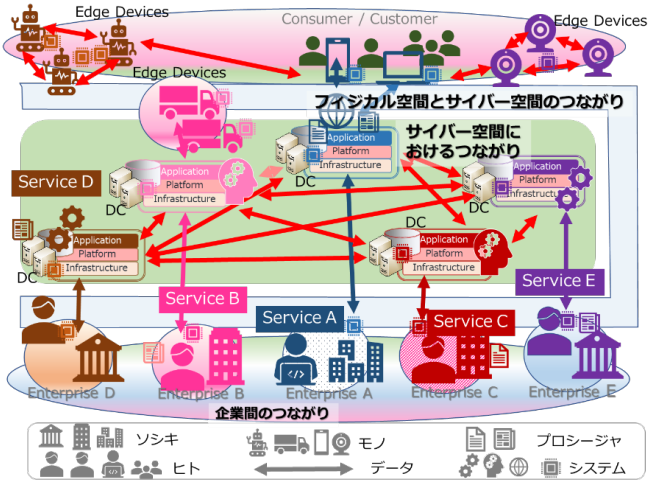
サプライチェーン管理の研究としては、契約にどのような形で役割と責任が記されているかの分析[2]や、米国政府調達基準となるNIST SP800-171の要求する高度なセキュリティに中小企業が対応する優先順序のCPSFを活用した検討[3]等の研究がある。また、Society5.0時代のガバナンスの研究としては、より多くの関係者の「幸福価値」に着目する[4]ものがある。サイバー空間とフィジカル空間の安心と安全については、セキュリティとセーフティを合わせて取り扱うリスクマネジメント手法[5]や、安全分析手法として注目されているSTAMP（System Theoretic Accident Model and Processes）/STPA（System Theoretic Process Analysis）[6]を使ったセーフティとセキュリティを統合したリスク分析手法[7]等が研究されている。我が国の組込みシステムの品質保証の研究には歴史があり、その成果が総合信頼性（dependability）の国際標準[8]となっており、これをセキュリティの保証に活用する研究もある[9]。本稿では、「バリュークリエイションプロセス」全体を俯瞰した実装イメージを検討した上で、これらの関連研究を参考に、CPSFの課題とその解決策を示す。

3．CPSFの概要

(1) 考え方

CPSFは、サイバー・フィジカルの世界を「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」、「サイバー空間におけるつながり」の3つの層と、「ソシキ」、「ヒト」、「モノ」、「データ」、「プロシジャー」、「システム」の6つの構成要素により整理して取り組むことを提唱している。CPSFの記述を参考に、例として、図表1にカメラ画像を自動認識し（Service E）、その結果を分析（Service C）して、倉庫からの自動出荷（Service D）と配送サービス（Service B）を連動させるような組み合わせサービス（Service A）を提供する架空の「バリュークリエイションプロセス」を示す。矢印の数と繋がりの組み合わせが、ソシキ、ヒト、モノ、データの複雑な関係、すなわち「サイバー攻撃の起点の拡大とその被害の影響の増大」のリスクを示している。無秩序に網状の接続が積み重なった場合には、それぞれの責任の分界点が不明確なだけでなく、全体像を把握することも困難になるだろう。

CPSFでは、「企業間のつながり」は、セキュリティポリシーの共有・実行を一体として行う組織のマネジメント、「フィジカル空間とサイバー空間のつながり」はサプライチェーンライフサイクル全体を通した、モノ、システムそのものの信頼性の確認、「サイバー空間におけるつながり」はサイバー空間におけるバリュークリエイションプロセスに関わるデータそのものの信頼性を確保するものとしている。そして、一つの組織が傘下の組織を垂直に統括管理するのではなく、それぞれの組織が信頼を確立し、信頼を確立した組織同士が横につながることで、安心と安全を確保しようという考え方を採用している。このため、バリュークリエイションプロセス全体のセキュリティ確保は、これまでのように組織のマネジメントの信頼性にのみ基点を置くのではなく、“各構成要素について必要なセキュリティ要件が満たされていることを確認”できる「信頼の創出」、信頼性リストへの登録と、それを確認した者以外の者による照会ができる「信頼の証明」、信頼の創出と証明を繰り返すことによる「信頼のチェーンの構築と維持」によるとされる。



図表1　バリュークリエイションプロセスのイメージ

(2) リスクの識別と対策要件

CPSFでは、JIS Q 31000:2010やJISQ 27001:2014等のリスクマネジメントにおける標準的なプロセスを使用して、このフレームワークを適用することを求めている。リスク源の洗い出しにおいて考慮すべき観点として、「バリュークリエイションプロセスに関わるステークホルダーとの関係」、

「IoT 機器を介したサイバー空間とフィジカル空間の融合」、「組織を跨るデータの流通」、「各層における信頼性の基点の確保」をあげ、三層構造モデルに基づいてバリュークリエイションを識別し、その構成要素に対するインシデントとその結果の事業への影響をもとにリスク分析を行えるように、各層毎に想定されるセキュリティインシデントが例示され、その対策要件がガイドされている。

(3) 対策要件と対策例

CPSF では、前述の各対策要件に対して、種々の基準へのリファレンスが示されている。そのリファレンスを見ると、CPSF の対策要件が米国の国立標準技術研究所（National Institute of Standards and Technology：以下 NIST）が作成したサイバーセキュリティフレームワーク 1.1 版の「対応（RS)」と「復旧（RC)」のプロセスを統合し、全ての内容を網羅したうえで、サプライチェーンリスク管理とデータセキュリティを中心に管理策を上乗せしたものになっていることがわかる。さらに、米国政府の調達先企業の一般的な情報管理に求められるセキュリティベースライン「NIST SP800-171」との関連付けや、国内のガイドラインである「サイバーセキュリティ経営ガイドライン Ver 2.0」、「IoT セキュリティガイドライン Ver 1.0」との関連も示され、国際基準との平仄やこれまでの取り組みで使用している各種基準からの継承性にも配慮されている。注目されるのは、「モノ、システムそのものの」に関するセキュリティの国際評価基準である Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5（以下 CC v3.1R5) のセキュリティ機能要件との関連が加えられていることである。脅威、脆弱性を考慮した評価や、認証・認可、暗号化等の実装においてより具体的な対応につながるものと考えられる。さらに、CPSF では「添付 C 対策要件に応じたセキュリティ対策例」として、このすべての対策要件に対する対策例が、＜ High-Advanced ＞、＜ Advanced ＞、＜ Basic ＞の三段階で示され、実装の際の優先順位付けに活用できるようになっている。

4．CPSF の実装と保証の課題

(1) バリュークリエイションプロセスの役割と責任の明確化

図表 1 に示した通り、バリュークリエイションプロセスの、ソシキ、ヒト、モノ、データが何の戦略もなく配置された場合、その繋がりの組み合わせは爆発的に多くなり、それぞれの「ソシキ」の責任の分界点が不明確になる。それぞれの「ソシキ」がそれぞれ自ら提供する製品・サービスについて責任を持つことが可能なアーキテクチャを確立し、これを共有・実行すべき「企業間のつながり（セキュリティポリシー)」とすることが、実装の第 1 の課題である。

(2) 効率的なセキュリティ実装による対応コストの削減と対応速度の向上

中小企業のセキュリティ対応への伝統的なアプローチは、身の丈に合わせた自助努力の範囲で「良いことにしてあげたい」というものである。しかしながら、バリュークリエイションプロセスにこのような弱小の「ソシキ」があれば、攻撃者の格好の標的になることは自明である。中小企業であっても、過剰な投資負担なしに、十分なセキュリティ対策をできるようにすることが、実装の第 2 の課題である。

(3) 調達者の要求が実装されていることの保証

CPSF が求める JIS Q 31000:2010 や JISQ 27001:2014 等の標準的なリスク管理プロセスは、「リスク」を提供側の組織の目的への影響の大きさの観点で評価・管理するプロセスであって、それを基点とした保証が、調達側からの要求や、個別のセキュリティ管理策のシステムへの実装を含むとは限らない。提供される保証が、サービスに対する「調達者の要求事項」の実装を確実に含むようにすることが、保証の第 1 の課題である。

(4) サービスの機能安全の保証

セーフティ（安全）は「機器やシステムが、人間の生活または環境に対する潜在的なリスク（ハザード）を緩和する度合い」であり、この安全を確保するためには、対象サービスのハザードを洗い出し、人命にかかわる可能性等、人間の生活または環境に対するリスクの大きさに応じて対応する必要がある。CPSF も、「機能安全の観点からの対策やサイバーセキュリティ対策を組み合わせて対応することが必要である。[10]」として関連する対策要件を示している。ハザードを分析して要求

事項を明らかにする手法、およびこれを保証する枠組みを確立することが、保証の第２の課題である。

(5) 変化対応が可能な保証の枠組み

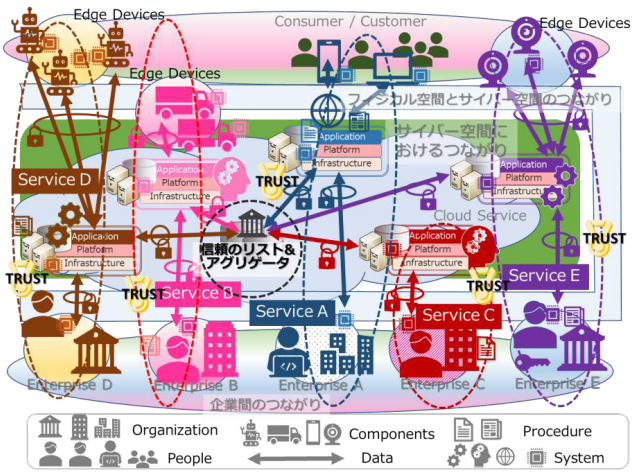
バリュークリエイションプロセスの提供するサービスは、「顧客にとっての価値」の変化に追随し続ける必要があり、これを提供するそれぞれのシステムも常に変更し続けなければ、バリュークリエイションプロセス全体の価値を維持できない。これまでの認証や監査 / 保証の枠組みは、過去の断面に対して評価を行うため、現在のシステムサービスとの乖離が避けられない。人手に依存したリスクアセスメントや契約、プロシジャーによる保証は、変化に柔軟に対応していくことが難しく、きめ細かく堅確に保証すればするほど、変化を伴うイノベーションを阻害する側面がある。サービスやシステムを動的に変化させつつ、その安心と安全が維持できていることを継続的に保証する手法の確立が、保証の第３の課題である。

5. 課題への対応とその実装の考察

(1) アグリゲート・コンピューティング・モデルによる役割と責任の明確化

TRON プロジェクトの提唱するアグリゲート・コンピューティング・モデル[11]は、ホームオートメーションを利用する「顧客」が、その裏側のサービスを理解して家電製品を選んだり、相互の通信設定を行ったりする必要がないように考案されたものである。エアコン、テレビ、オーディオ機器、洗濯機などの家電メーカーが自社の家電との通信を一元的に担い、自社の家電のライフサイクル管理に責任を持つ。他社の家電との連携は IoT-Aggregator という中継者がそれぞれの家電の提供者を識別し、オープン API の仲立ちをすることで実現する。「信頼の創出」は各メーカーが行い、IoT-Aggregator という信頼性リストへ登録し、IoT-Aggregator の「信頼の証明」を介して「信頼のチェーンの構築と維持」を行うのである。

図表２に図表１の事例に対してアグリゲートコンピューティングモデルを適用したものを示す。「ヒト」と「モノ」を結ぶ矢印がいずれかの「ソシキ」の管理下となり責任範囲が明確にできる。技術的には、個々の「モノ（家電等機器）」をクラウドにトンネリングでセキュアに直結することで、提供メーカーがクラウドサービスを経由して「総体として」サービスを提供するアーキテクチャを実現する。これにより、「ソシキ」は自社サービスの「モノ、システムそのものの信頼性の確認」について、そのライフサイクルを通じて責任が持てるようになる。それぞれの「モノ（IoT 機器の実身）」に対応したクラウド上の「仮身（仮想デバイス）」が、「システム」との通信を行うので、データの転写機能の信頼性を確保するための管理・監視も「ソシキ」の責任の下で容易に行える。「ソシキ」の信頼を記録した「信頼のリスト＆アグリゲータ」がそれぞれの機器とサービスを識別して仲介することで「信頼のリスト」の抜けや漏れを防ぐことができ、API を仲立ちすることで厳密なデータの標準化なしに異なるサービス提供者間の相互運用性を確保することができる。すなわち、「バリュークリエイションプロセスに関わるデータそのものの信頼性」を確保した「サイバー空間におけるつながり」が可能になる。「ソシキ」はこの「信頼のリスト＆アグリゲータ」を介して繋がるので、そのバリュークリエイションプロセスのセキュリティポリシーがそれぞれの「ソシキ」に自動的に適用される。アーキテクチャが「セキュリティポリシーの共有・実行を一体として行う」ことを実現する「ガバナンス・バイ・アーキテクチャ」である。



図表２　アグリゲート・コンピューティング・モデルの CPSF 適用

「信頼のリスト」をもとに通信を仲介する「信頼のリスト＆アグリゲータ」は、多様なサービスを抽象化して使い易くする効果も期待でき、サイバー空間における新たなサービスを促進する基盤となる可能性がある。例えば「生活支援ロボ」、「自

動検診」、「ヘルスデータ管理」、「介護ロボ」等を実現する、「医療・介護用のアグリゲータ」を設けると、これらの新しい組み合わせの実現が飛躍的に容易になり、新しい「バリュークリエイションプロセス」が数多く生み出せるようになるだろう。

(2) セキュリティ実装コードの共有等による安価で高速なサービス創出

米国では NIST がセキュリティベンダーと協働して市販のテクノロジーを使用したモジュール式の簡単に適応可能なサイバーセキュリティソリューションを開発し、SP1800 シリーズ（図表 3）[12] として無償で公開している。このシリーズでは電力会社向けの監視システムや、メールセキュリティ、IT 資産管理等の具体的なセキュリティを実現するために使用する市販製品とその実装のためのコードがガイドされている。

Number	Title	Technology Partner/Collaborato
1800-17	Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers	RSA, Splunk, StrongKey, TokenOne, Yubico
1800-14	Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation	AT&T, CenturyLink, Cisco, Comcast, Juniper Networks, Palo Alto Networks, The George Washington University
1800-12	Derived Personal Identity Verification (PIV) Credentials	Entrust Datacard, Intel Corporation, Intercede, MobileIron, Verizon
1800-8	Securing Wireless Infusion Pumps in Healthcare Delivery Organizations	Baxter Healthcare Corporation, B. Braun Medical Inc., Becton, Dickinson and Company (BD), Cisco, Clearwater Compliance, DigiCert, Hospira Inc., a Pfizer Company (ICU Medical), Intercede, Medical Device Innovation Safety & Security Consortium (MDISS), PFP Cybersecurity, Ramparts, Smiths Medical, Symantec Corporation, TDi Technologies, Inc.
1800-7	Situational Awareness for Electric Utilities	Dragos, Hewlett Packard Enterprise, ICS2, OSIsoft, Radiflow, RS2 Technologies, RSA a Dell Technologies business, Schneider Electric, Siemens, TDi Technologies, Waratek, Waterfall Security Solutions
1800-6	Domain Name System-Based Electronic Mail Security	Fraunhofer IAO, Internet Systems Consortium, Microsoft Corporation, NLNet Laboratories, Secure64
1800-5	IT Asset Management	AlphaPoint Technology, Belarc, Computer Associates, Microsoft, Peniel Solutions, PI Achievers, PuppetLabs, RedJack, Splunk, Tyco, Vanguard Integrity Professionals
1800-4	Mobile Device Security: Cloud and Hybrid Builds	Intel, Lookout, Microsoft, Symantec
1800-2	Identity and Access Management for Electric Utilities	AlertEnterprise, CA Technologies, Cisco Systems, GlobalSign, Mount Airey Group (MAG), Radiflow, RSA, RS2 Technologies, Schneider Electric, TDi Technologies, XTec
1800-1	Securing Electronic Health Records on Mobile Devices	Cisco, IBM, Intel, MedTech Enginuity, Ramparts, RSA, Symantec

図表 3　SP1800 シリーズで提供されている実装用のガイダンス

[Source] The National Institute of Standards and Technology. NIST Special Publication 1800-series General Information. NIST. (オンライン) (引用日 : 2020 年 3 月 3 日 .)
https://www.nist.gov/itl/nist-special-publication-1800-series-general-information.

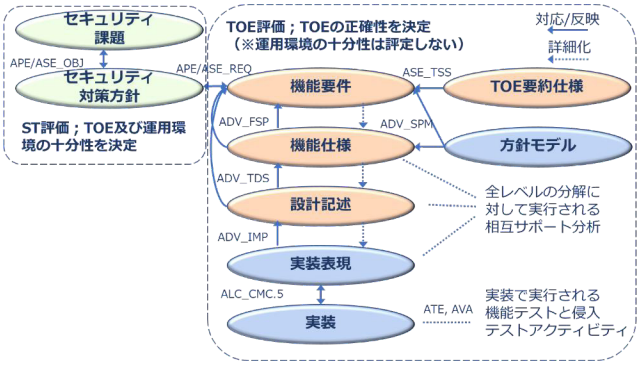
このように無償または格安で使えるセキュリティが、中小企業を含めた「バリュークリエイションプロセス」の信頼を確立するために必要である。ソフトウェアコードはいくらコピーしても劣化することはない。例えば企業グループや業界、政府・行政機関等が、クラウド環境において、この様なコードや、それを実装したサービスを格安で共用することを推進することは、社会全体のセキュリティを効率的に底上げすることにつながるだろう。セキュリティ水準は常により高いものが求められるように変化し続けている。高い水準で実装することは、将来に備えた余力であり [13]、過剰品質ではない。なるべく多くの組織同士が、実装可能なセキュリティのためのコードやサービスを共有することで、社会全体が高度で効率的なセキュリティを実現することが国や産業の競争力につながる。高度なサイバー・フィジカル・セキュリティを、安価に提供する新しい「バリュークリエイションプロセス」を創出することが必要に思える。

(3) 調達者の要求事項の観点でのサービスの保証

「バリュークリエイションプロセス」の安心と安全の保証には、「各構成要素について必要なセキュリティ要件が満たされていることを確認」することが必要であり、これには製品のセキュリティを保証するための CC v3.1R5 の枠組みを使うことが有効と考えられる。CC v3.1R5 は「概説と一般モデル [14]」「セキュリティ機能コンポーネント [15]」「セキュリティ保証コンポーネント [16]」の 3 つのパートから構成された ISO 規格であり認証制度も用意されている。

この規格では、評価対象（TOE）に対する調達者の要求事項（PP）[TOE の定義、環境、対策方針、要件、根拠] に基づき、セキュリティ目標 (ST)[TOE の定義、環境、対策方針、要件、要約仕様、PP との整合性、根拠] を設定し、「セキュリティ機能コンポーネント」、「セキュリティ保証要件」、「評価保証レベル」の 3 軸で評価する。

この基準に基づいて評価することにより、図表 4 に示す通り、調達者の要求事項に対して、どのようなセキュリティ要件を設定したか (ST 評価)、どの機能コンポーネントを実装したか（セキュリティ機能コンポーネント）、そして、その開発と



図表 4　CC v 3.1R5 による実装の保証概要

[Source]https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf, p84 図 11 ADV: 構造間及びそれらと他のファミリ関係

運用がどのレベルで行われているか（セキュリティ保証要件）、さらにこの実装の確認をどの程度厳格に行ったか（評価保証レベル）を示すことができる（TOE 評価）。

なお、CC v3.1R5 は各国の調達基準にも採用されているが、せっかく認証を取得してもシステムをわずかでも変更すると、そのたびに取り直す必要があるなど使い勝手が悪い面があり、後述のように、この活用にはこれを自動化して効率化する等の工夫が必要となる。

(4) ハザードアセスメントとセキュリティ／セーフティ・バイ・デザイン

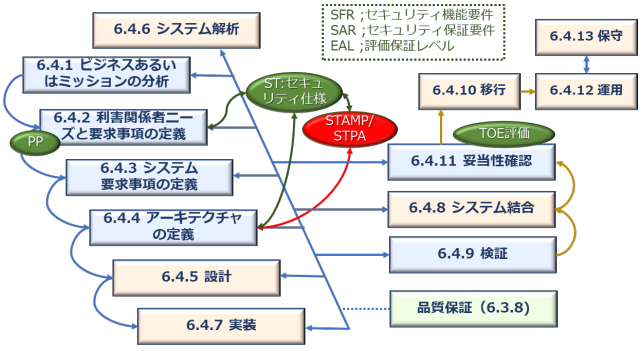
「バリュークリエイションプロセス」のリスクがハザードにつながりうるものである場合には、関連研究で参照した、セキュリティとセーフティを合わせて取り扱うリスクマネジメント手法 [5] や、安全分析手法として注目されている STAMP/STPA を使った、セーフティとセキュリティを統合したリスク分析手法 [6] 等への取り組みが必要になる。STAMP は、「コンポーネント」と「相互作用（コントロールアクションとフィードバック）」に着目してメカニズムを説明するモデルであり、STPA はこのモデルをもとにした安全解析手法で、コントロールアクション（安全確保に必要な指令）について、「①与えられない場合のハザード」、「②誤った内容が与えられたが場合のハザード」、「③早すぎたり、遅すぎたり、順序誤りの場合のハザード」、「④短すぎたり長すぎたりした場合のハザード」に分けて、分析の漏れを防ぎ、流れを整理したものである。図表 5 では A から C の 3 つのコンポーネント間において、機能安全のためのコントロールアクションであるコマンド 1 から 3 に問題が生じた場合の安全制約が示されている。コマンド 1 が発行されない場合と、異常なタイミングで発行された場合、およびコマンド 2 が異常なタイミングで発行された場合にハザードに至る。このケースを発生させる機能に対して、必要なセキュリティ対策機能を選定し、厳重な品質管理を実施して実装を行っていくことになる。

コントロールアクション	非安全なコントロールアクション			
	コントロールアクション無し	コントロールアクションあり		
		内容が誤り	内容は正しい	
			早すぎ、遅すぎ、順序誤り	早すぎる停止、長すぎる適用
コマンド 1	ハザード 1 に至る（UCA 1）	該当なし	ハザード 2 に至る（UCA2）	該当なし
コマンド 2	該当なし	該当なし	ハザード 3 に至る（UCA3）	該当なし
コマンド 3	該当なし	該当なし	該当なし	該当なし

図表 5　STAMP/STPA による
安全解析の例による安全解析の例

[Source] 独立行政法人 情報処理推進機構システム安全性解析手法 WG. はじめての STAMP/STPA ～ システム思考に基づく新しい安全性解析手法～ . 情報処理機構 社会基盤センター . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.ipa.go.jp/files/000051829.pdf. 図 1.1-1

STAMP/STPA は、「バリュークリエイションプロセス」における自社サービスの重要なコンポーネントが、他社のサービス等との連携の際に、必要なコントロールアクションが来なかったり、誤っていたりしたときに、ハザードに至るような条件がないかどうかを洗い出し、ハザードに至る組み合わせを特定して安全を確保するために使用できる。図表 6 にこれをセキュリティ / セーフティ・バイ・デザインに組み込んだ開発の流れのイメージを示す。セキュリティとセーフティの機能とその重要度は、システムの物理構成や論理構成の変更にともなって必ず見直しが必要になるので、セキュリティ / セーフティ・バイ・デザインを実現するためには、アーキテクチャ定義 (6.4.4) のアウトプットであるシステムの物理構成や論理構成を、利害関係者ニーズと要求事項の定義 (6.4.2) にフィードバックし、必要な「機能コンポーネント」を選定してセキュリティ目標（ST）を作成し、「セキュリティ保証要件」をシステムライフサイクルに組み込み、必要とする「評価保証レベル」を定めてモノ作りのプロセスに反映する。セーフティについては、STAMP/STPA 等で明らかになったハザードの深刻さに対してセキュリティ目標（ST）を作成し、以後はセキュリティと同じ流れで実装する。

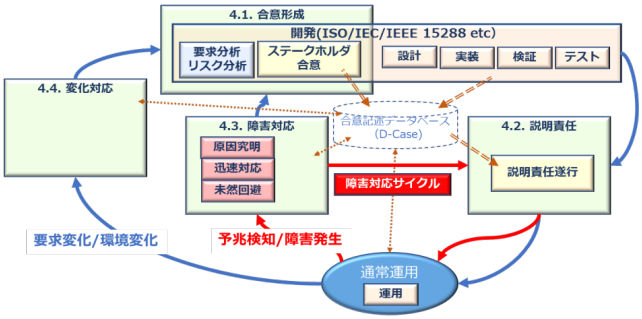


図表 6　セキュリティ セキュリティ /
セーフティ・バイデザインの確立

[Source] ソフトウェア高信頼化センター (SEC), 成功事例に学ぶシステムズエンジニアリグ～ IoT 時代のシステム開発アプローチ～ , 独立行政法人情報処理推進機構 (IPA), 2018, https://www.ipa.go.jp/files/000064704.pdf, を参考に作成

(5) 開放系総合信頼性技術（IEC62853）の活用と自働化による変化への対応

開放系総合信頼性技術（IEC62853）[17] は、要求についてのステークホルダーとの合意を記録し、開発の結果がその合意を満足することのエビデンスを記録することで、説明責任を果たし続けるライフサイクルプロセスを実現し、長期間使われる IoT 機器を陳腐化させないように開発された。関連研究で参照したように、これをセキュリティの保証に活用すること [9] も研究されている。図表 7 に開放系総合信頼性技術による変化対応の流れを示す。システムのライフサイクルを通して、セキュリティ / セーフティの説明責任を果たすために必要な「要件 / 合意」と、それが実現されていることを示すテスト / 検証の「エビデンス」が「合意記述データベース」に記録され続ける。



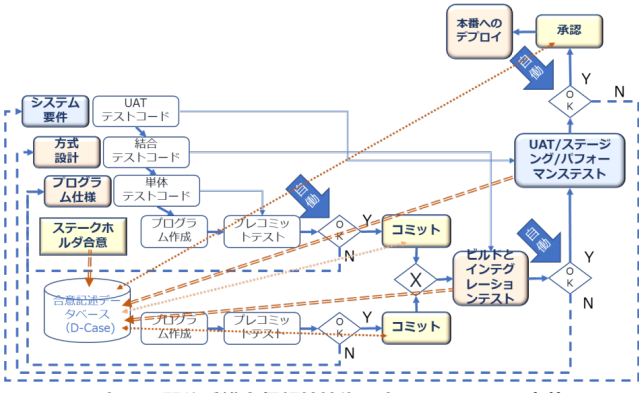
図表 7　開放系総合信頼性技術による変化対応

[Source] 一般社団法人ディペンダビリテ技術推進協会部会 , はじめてみる IEC62853 の実装 , The Association of Dependability Engineering for Open Systems. (オンライン) (引用日 : 2019 年 10 月 7 日 .) http://deos.or.jp/link/obj/pdf/Introduciton62853Implementation-DEOS20180605.pdf. P10 図 2.8 を参考に作成

システムを本番にリリースするためには、受け入れ確認テストに合格することが必要である。受入確認テストの内容が合意できないものは、要件の満足を確認する手段がないので要件とは言えない。実務では契約上の都合から要件の詳細検討を先送りし、テストができない抽象度の高い文章を要件と称しているものをしばしば見かけるが、実際には受入確認テストが合意できなければ、要件を完全に合意したことにはならない。ここでは、受入確認テストの内容を合意事項とし、自動化に組み込んだ場合の対応を示す。

開放系総合信頼性技術の変化対応の枠組みは DevOps で使用される CI/CD（継続的インテグレーション／継続的デリバリー）のパイプラインと類似する。図表 8 は開放系総合信頼性技術を DevOps へ実装したイメージである。受入確認テスト (UAT) を含めて自動化されることにより、要件変更に早く確実に対応できるようになるだけでなく、単体や結合レベルの変更が何回生じても、本番にリリース可能な品質が確保できているか否かが直ちに確認できるようになる。

この自動化が実現すると、CPSF の対象とする「プロシジャー」の多くは、DevOps の管理システムが実行する「コード」に置き換わる。このことは、ヒューマンエラーを排除して品質とその信頼性を格段に向上させることができる。この「コード」の内容や実行記録を継続的にモニタリングし、それを監査することにより、要件を満たしたサービスが提供されていることをより確実に保証することができるようになる。



図表 8　開放系総合信頼性技術の DevOps への実装

[Source]Len Bass. Ingo Weber. Liming Zhu, DevOps 教科書 (Kindle 版), 日経 BP 社 ,2016 年 , 位置 No.2004 図 5.1 を参考に作成

6.「バリュークリエイションプロセス」の保証と監査

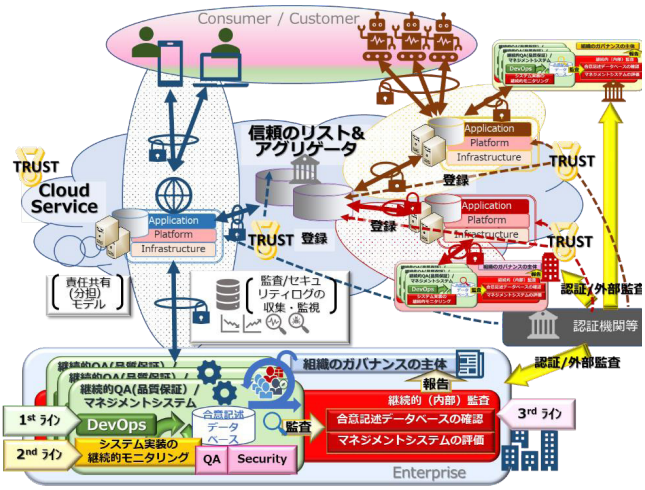
(1) 三線防御を基礎とする信頼のチェーン構築と継続的監査の実現

「ソシキ」の責任範囲が明確になれば、それぞれの「ソシキ」が明確になった責任範囲について三線防御などのフレームワークで統制を確保し、それを信頼し合うことが可能になる。図表 9 にそれぞれの組織が自らのサービスに信頼を得て信頼のチェーンを構築し維持する枠組みのイメージを示す。

「バリュークリエイションプロセス」の「信頼の創出」は 1st ラインの CI/CD(継続的インテグレーション／継続的デリバリー) と 2nd ラインの継続的モニタリング、および 3rd ラインの継続的監査が一体となって実現する。セキュリティとセーフティの実装と実施は 1st ラインの責任であり、サービスの開発と運用を確りと実施してそのエビデンスを記録する必要がある。この実現のためには、

CI/CD の枠組みを導入して開発からリリースまでの一連の流れを自動化し、記録を取り続ける必要がある。CPSF の要求する組織全体のリスクマネジメントとの整合性の確保は 2nd ラインが実行責任を負う。品質保証(QA)プロセスやセキュリティの継続的モニタリングによって検知した問題について直ちに対応していなければならない。内部監査は 3rd ラインとして、これらの状況の継続的監査を行い、組織のガバナンスの主体と、認証機関や外部監査に対して説明可能な監査報告を作成する。この監査報告とそのエビデンスによって客観的に確認可能となった「ソシキ」の統制活動が、各「ソシキ」の「信頼の証明」を可能にする。この組織の統制活動とエビデンスを認証機関や外部の監査法人等が確認して「信頼のリスト」に登録し、「信頼のリスト」に登録されている組織同士が繋がりあうことで、「信頼のチェーンの構築と維持」が実現する。

これまでのオンプレミス環境でのソフトウェア開発では、このように開発から運用までを一連で自働化し、継続的モニタリングや継続的監査を実現するためには、多数のツールを購入して接続する必要があり、費用や技術の観点で難しい面があった。しかし、今日のクラウドサービスの多くでは、CI/CD はもはや常識として実装が進んでおり、クラウドを利用する組織がデータやアクセスの管理、アプリケーションの設定などの「クラウドにおけるセキュリティ」を容易に監視できるように、継続的モニタリング、継続的監査等の自動化を実現するためのツールもあらかじめ多数準備されており、実現の環境は既に整っていると言える。



図表９　三線防御を基礎とする信頼のチェーン構築維持

(2) 品質保証（QA）と監査人の技術

これまで見てきたように、“各構成要素について必要なセキュリティ要件が満たされていることを確認”するためには、「調達者の要求事項の観点でのサービスの保証」や「機能安全の保証」が必要であり、このために監査人は、その実現技術を理解した上で評価する必要がある。

ソフトウェア・ライフサイクルの国際規格である ISO/IEC/IEEE12207 は 2017 年に改訂され、従来の「ソフトウェア監査プロセス (7.2.7)」は「ソフトウェア品質保証プロセス (7.2.3)」と統合され、「品質保証プロセス (6.3.8)」になっている [18]。このプロセスが定義する Outcomes (プロセスが成功した成果) では、「プロジェクトの製品、サービス、プロセスの評価が実行され、品質管理のポリシー、手順、要件と一致している」こと、「品質保証手順が定義され、実装されている」こと、「品質保証評価の基準と方法が定義されている」こと、「問題には優先順位付けされて対応されている」こと、「インシデントが解決されている」こと、「評価結果が関連する利害関係者に提供される」ことがあげられている。同規格の監査 (audit) の定義は「仕様，標準，契約合意，又は他の基準への適合性をアセスメントするための作業成果物又は作業成果物の集合に対する独立した審査」[19] である。監査人がこれを実践するためには、これまで見てきたようなクラウドを活用した新しいアーキテクチャと、複雑化したシステムにおける品質保証技術を理解し、これらの「作業成果物」を評価できるようになる必要がある。

7. 結論

CPSF が提唱する、サイバー・フィジカルの３つの層と、６つの構成要素のガバナンスのために、アグリゲート・コンピューティング・モデルをアーキテクチャとして採用することで、複雑なバリュークリエイションプロセスの関係の複雑化を防ぎ、各組織の責任分界点を明確にできる。

これからのサプライチェーン管理で最も重要となる、「中小企業を含めた」バリュークリエイションプロセス全体の安全確保のためには、中小企業向けに無理にハードルを下げた基準を作るのではなく、可能な限り高度なセキュリティをコードレベルでシェアすることなどにより、コミュニティや社会全体でセキュリティのためのコストを分担して負担していくことが必要である。

“各構成要素について必要なセキュリティ要件が満たされていることを確認”するためには、STAMP/STPA や CC v3.1R5、開放系総合信頼性技術等の「品質保証技術」が役に立ち、これらの手法を CI/CD に組み込んで自動化を図ることは、信頼性の高いサービス構築を可能とするとともに、要件の変更に強いソフトウェア開発の実現にもつながる。

信頼のチェーンの構築は、それぞれの組織が CI/CD、継続的モニタリング、継続的監査等において、エビデンスによって客観的かつ継続的に確認可能な統制活動を行い、これを認証機関や外部の監査法人等が確認して「信頼のリスト」に登録することで実現する。監査人はこの実践のため、クラウドを活用した新しいアーキテクチャと、複雑化したシステムにおける品質保証技術を理解し、その「作業成果物」を評価できるようになる必要がある。

8. おわりに

Society5.0 は、我が国が、少子高齢化や地域、年齢、性別、言語等による格差の課題先進国として世界に先駆けて模範となる未来社会を示そうというものである [18]。CPSF は、これを実現するために国際基準を上回る水準を目指している。これは数十年前に日本が品質管理への取り組みを始めた原点と同じ精神である。日本の高度成長を支えた「日本的品質管理」は、日本製品の品質が全く世界に太刀打ちできなかった当時、なんとか世界水準に追いつきこれを追い越そうと組織を越えて研究と実践を積み上げた成果であり、決して垂直統合で傘下企業を統制して実現したものではない。当時は中小企業を含めたサプライチェーンの参加者全員が、自律的にそれぞれの責任の範囲の品質保証に取り組み「買い手と売り手の品質管理的十原則」[19] に代表される信用できるサプライチェーンを一丸となって目指したのである。幸いなことに TRON や DEOS 等、この領域の世界標準として認められた日本発のオープンテクノロジーは実は意外に多い。これらの知財を活用し、CPSF に日本のモノ作りの精神と技術を生かして正面から取り組むことが、Society5.0 の目指す経済的発展と社会的課題の解決に直結するものと考える。

(参照文献)

1. 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 . 経済産業省 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf.

2. 森 淳子 , ほか . IT サプライチェーンの責任範囲の実態から見た対策強化のための提案 .　: 情報処理学会 , Computer Security Symposium 2019, 2019, pp98-105.

3. 中川 哲 , 後藤厚宏 . 中小企業に NIST SP800-171 準拠を求めた場合の課題と解決策 .　: 情報処理学会 , 2020, pp1-8.

4. 小原重信 . 個人の幸福価値に対する社会共感と P2M プログラムガバナンス .　: 国際 P2M 学会 , 2018, pp325-344.

5. 五郎丸 秀樹 . IoT と CPS 時代の新たなリスク管理手法の調査 . 2018, pp1-8.

6. 独立行政法人 情報処理推進機構システム安全性解析手法 WG　. はじめての STAMP/STPA 〜システム思考に基づく新しい安全性解析手法〜 . 情報処理機構　社会基盤センター . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.ipa.go.jp/files/000051829.pdf.

7. 金子 朋子 , ほか . STAMP S&S 〜システム理論によるセーフティ・セキュリティ統合リスク分析 .　: 情報処理学会 , 2019, pp41-47.

8. 木下佳樹 , ほか . 開放系総合信頼性の標準化〜 CREST 研究プロジェクトと IEC 標準化の相互作用〜 .　: 情報処理学会 , 2019, pp35-52.

9. 金子 朋子 , ほか . セキュリティ要求分析・保証の統合手法 CC-Case の有効性評価実験 .　: 情報処理学会 , 2018, pp11-26.

10. 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 . 経済産業省 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf, p44.

11. 坂村健 . オープン IoT- 考え方と実践 .　: パーソナルメディア社 , 2017, 位置 No.592.

12. The National Institute of Standards and Technology. NIST Special Publication 1800-series General Information . NIST. (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.nist.gov/itl/nist-special-publication-1800-series-general-information.

13. AI プロダクト品質保証コンソーシアム . AI プロダクト品質保証ガイドライン . QA4AI. (オンライン) (引用 日 : 2019 年 10 月 7 日 .) http://www.qa4ai.jp/QA4AI.Guideline.201905.pdf,p2-16.
14. ISO/IEC. 情報技術セキュリティ評価のためのコモンクライテリア　パート 1: 概説と一般モデル(IPA 訳). 情報処理推進機構 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.ipa.go.jp/security/jisec/cc/documents/CCPART1V3.1R5-J1.0.pdf.
15. —. 情報技術セキュリティ評価のためのコモンクライテリア　パート 2: セキュリティ機能コンポーネント . 情報処理推進機構 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.ipa.go.jp/security/jisec/cc/documents/CCPART2V3.1R5.pdf.
16. —. 情報技術セキュリティ評価のためのコモンクライテリア　パート 3: セキュリティ保証コンポーネント . 情報処理推進機構 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf.
17. ディペンダビリティ技術推進協会　技術部会　標準化部会 . はじめてみる IEC62853 の実装 . 一般社団法人　ディペンダビリティ技術推進協会 . (オンライン) (引用日 : 2019 年 10 月 7 日 .) http://deos.or.jp/link/obj/pdf/Introduciton62853Implementation-DEOS20180605.pdf.
18. ISO/IEC/IEEE. Annex I　Process Mapping from ISO/IEC/IEEE 12207:2008. ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes.　: ISO, 2017, p.130.
19.　—. ISO/IEC/IEEE 12207:2017 Systems and software engineering　— Software life cycle processes. : ISO, 2017, p3.
20. 内閣府 . Society 5.0. 科学技術政策 . (オンライン) (引用日 : 2019 年 10 月 07 日 .) https://www8.cao.go.jp/cstp/society5_0/.
21. 石川馨 . 日本的品質管理—TQC とは何か 増補版 .　: 日科技連 , 1984, pp228-229.