CPSEC-WP-2019002

サプライチェーンにおける信頼構築に向けて
－ 第 2 報 信頼構築技術について －

2020 年 1 月

国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究センター

［概要］ 近年、製品・サービスのサプライチェーンにおいて、製品・サービスへの信頼を損なう事故（セキュリティ事故を含む）が数多く報告されている。本報告は、「サプライチェーンにおける信頼構築に向けて」と題するホワイトペーパーの第 2 報として、これらの事故を防止する「信頼構築技術」を説明する。

はじめに、信頼構築の基本的考え方を紹介し、信頼構築のための要求と証拠の提示について詳しく説明する。次に、信頼構築の技術的プロセスの中核である「信頼の創出」と「信頼チェーンの構築」の実現技術を説明する。さらに本技術の効果について、事故事例を参照して説明する。最後に、我々の信頼構築の基本方針が、これまでに情報技術分野で示された「信頼」と同じ考え方に立つことを説明する。

1. 信頼構築の基本的考え方

近年、サーバやルータなどの情報通信機器をはじめ、自動車・鉄道・建築物などの社会インフラまで、様々な産業分野で、製品・サービスに対する信頼を損なう事故（セキュリティ事故を含む）の発生が報告されている。

貿易や物流のグローバル化に連れて、製品やサービスのサプライチェーン（以下、SC と略記する）は、より大規模化し複雑化している。また、情報技術(IT)の進歩に伴い、IoT(Internet of Things)の概念が現実のものとなり、サイバーフィジカルシステム（以下、CPS と略記する）と呼ばれる情報通信システムと機械システムとが高度に組み合わされたハイブリッドなシステムの普及が本格化しつつある。

これらグローバル SC に対応するシステムでは、大規模化や複雑化に伴い、製造・運用における障害や故障の発生確率が高まり、システムの信頼を損うリスクの増加が懸念される。また CPS では、アタックサーフェス（攻撃の標的となり得る対象の全体）が増えることから、サイバー攻撃を受ける可能性が高まることが指摘されている。

第 1 報[1]では、CPU ボードや食品、航空機運行等の様々な製品・サービスを対象に、SC の信頼を損なう事故事例を調査した。収集した事例を分析した結果、それらに共通する特徴として下記を得た。

［SC 事故事例の特徴］

(1) 事故は、製品・サービスの設計、調達、製造、流通、運用に係る業務プロセスの実行に際して、必要な規程に不備があったためか、または規程に違反したためか、のいずれかの理由で起こる。

(2) 事故原因の作り込みと事故発生は、SC のどの業務プロセスでも起こる可能性がある。また、事故原因の作り込みと事故発生は、異なる組織で起こる可能性がある。

さらに第 1 報では、上記分析結果に基づき、図 1 に示す SC の信頼構築を実現する基本的考え方を提示した。

(1) 組織間の信頼構築

製品やサービスを授受する組織間の信頼は、発注側組織が製品に対する信頼や機能に係る要求を提示（図 1 の「信頼要求提示」）し、受注側組織が自らのプロセスがその要求に足ることの証拠を、必要に応じて、データをもって提示（図 1 の「証拠提示」）することで構築される。本書では、機能だけでなく信頼に関する要求も含めた要求を信頼要求と呼ぶ。

(2) SC 全体の信頼構築

SC 全体を通しての製品やサービスの信頼は、SC の参加組織が、組織間の信頼を繋げていくことで構築（図 1 の「信頼チェーンの構築」）される。

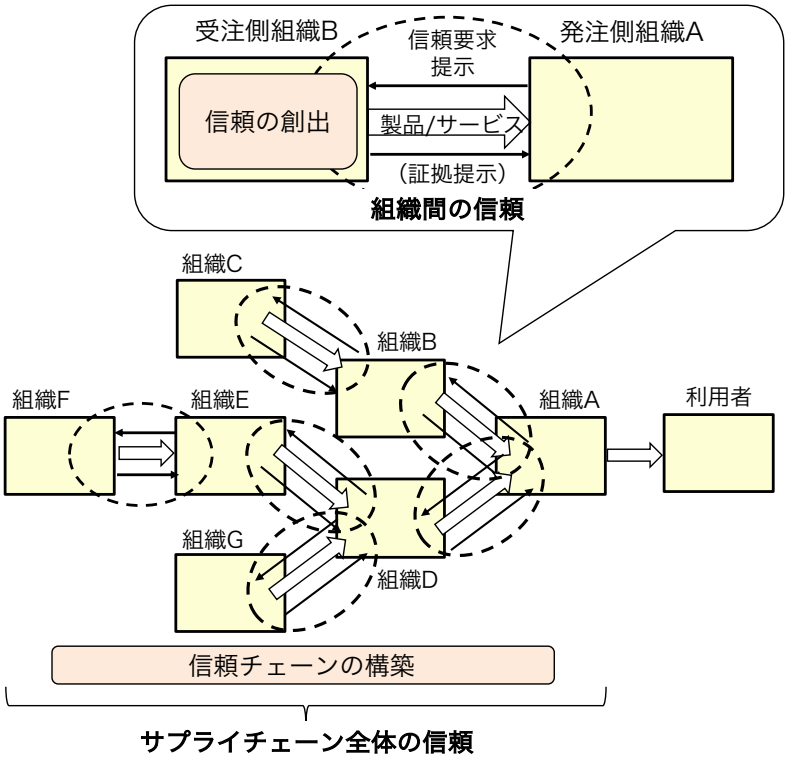

図 1 信頼構築の基本的考え方

以下では、上記の基本的考え方を実現する信頼構築技術を構成する。2 章では、製品やサービスに関する信頼構築の基本的考え方のカギとなる「信頼要求提示」と「証拠提示」、および「サプライチェーン全体の信頼の構築」について説明する。やや詳細な議論を含むので、必要に応じて読み進められたい。3 章では、SC の各組織における「信頼の創出」の技術プロセスを説明する。4 章では、SC 全体での「信頼チ

ェーンの構築」の技術プロセスを説明する。

2. 信頼の構築に関する考察

2.1. 発注側組織の信頼要求提示

発注側組織は、調達する製品やサービス（以下、製品と略記する）について、1 で述べたように、「信頼要求」を提示する。信頼要求に含まれる通常の要求には、機能や性質に関して必要な様々な要求が含まれる。

信頼要求に含まれる信頼に関する要求は、発注側組織が必要とする製品の機能や性質が、どの程度の確かさで提供されるか、に関する要求である。例えば製品が暗号モジュールである場合、技術的要求として、国際標準規格 ”ISO/IEC 19790: 2012 セキュリティ技術 – 暗号モジュールのセキュリティ要求事項” が挙げられる。この規格が規定する技術要求事項が正しく設計され、実装されたことの保証を求める要求は、信頼に関する要求である。

技術要求とは別に、第 1 報の事故事例の分析結果が示すとおり、製造業務では、製品を製造・運用する方法・機器・人員等の管理規程の遵守が重要となる。管理規程として、セキュリティ分野では “ISO/IEC 27001: 2013 セキュリティ技術 – 情報セキュリティマネジメントシステム– 要求事項”があり、品質管理分野では “ISO 9000 品質マネジメントシステム” が挙げられる。これらの管理規程に従って製造されたことの保証を求める要求も信頼に関する要求である。

なお上記の例は、すべて国際標準規格であるが、要求として業界標準規格が用いられる場合がある。また、国際標準規格や業界標準規格のような公開規格情報ではなく、発注側組織と受注側組織間の契約に付随する非公開の取り決めとして、要求が提示される場合もある。

2.2. 受注側組織の証拠提示

受注側組織は、発注側組織の信頼要求を満たす製品を製造する。さらに受注側組織は、製品等が要求を満たすように製造されたことの証拠を提示する。本節では、この製造と証拠提示のために、受注側組織が実行する処理を図 2 に従い説明する。

第 1 の処理は、製品の要件の抽出（図 2 の 1.）である。受注生産品であれば、受注側組織は 2.1 の発注側組織の信頼要求に従って製品の要件を作成する。市販品や民生品であれば、受注側組織は製品製造者としての「製品仕様」を有する。この製品仕様、あるいは発注側組織の信頼要求に基づいて、製品に対する要件定義書を作成する。

第 2 の処理は、要件の分析（図 2 の 2.）である。受注側組織は、要件定義書の要件通りの製品を製造するために、「誰または何が、何を、どのように、どの程度まで、処理するか」について、実施可能なレベルにまで詳細化した作業規程を作成する。さらに受注側組織は、作業規程通りに製造したことの証拠データとして、何を測定して保存すべきかを決定する。

第 3 の処理は、作業規程の合意（図 2 の 3.）である。受注側組織は、発注側組織と協議して、作成

した作業規程が発注側組織の信頼要求を満たす内容であることを確認して、作業規程の内容について合意を得る。

第 4 の処理は、製品の製造・検査（図 2 の 4.）である。製造・検査担当者は、作業規程に従って製品を製造・検査し、その証拠を保存する。受注側組織は、発注側組織に製品を出荷し、証拠を提示する。

なお、受注側組織は、保存した証拠データのうち、自社の事業的制約を考慮して、発注側組織に開示可能な証拠を制限する場合がある。例えば、作業規程自体が、組織固有のノウハウであり事業上の秘密である場合、作業規程が明らかとなる証拠データは開示できない。受注側組織は、上記の作業規程の合意の処理で、開示する証拠データの妥当性について、発注側組織と事前に合意しておく必要がある。

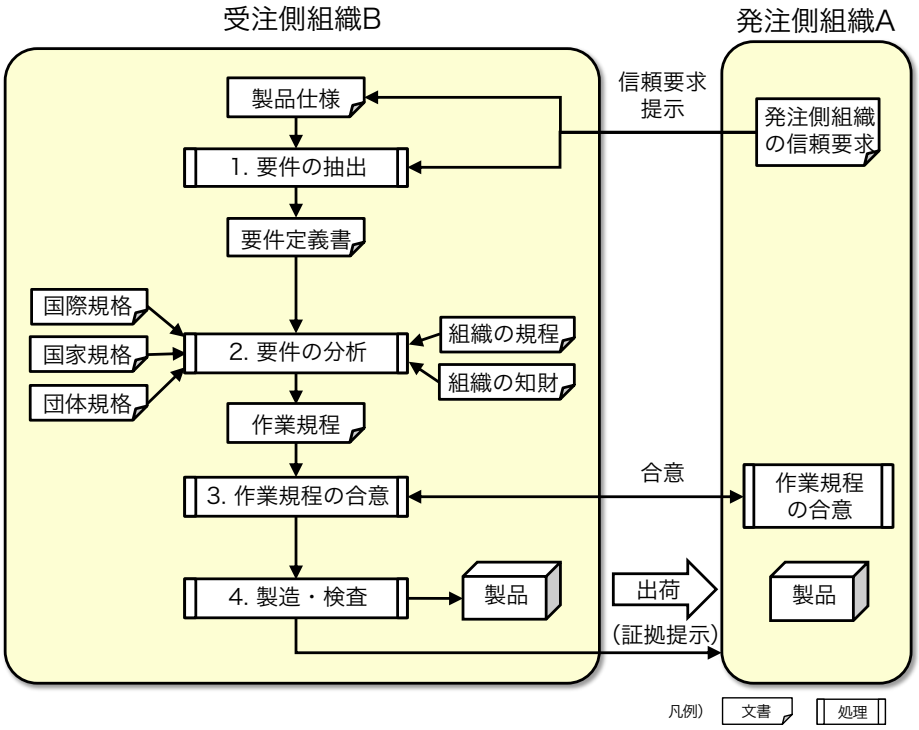

図 2　受注側組織による要件の分析

2.3.　サプライチェーン全体の信頼の構築

図 1 は、例えば、組織 A が製造する最終製品は、組織 B～F が提供する部品や製品によって構成されていることを示している。1.で述べたように、各組織は、部品や製品の発注と納入に当たり、信頼要求提示と信頼提示によって、組織間の信頼を構築する。そして、サプライチェーン全体にこの関係を構築することによって、サプライチェーン全体の信頼が構築される。このことは、視点を組織から製品や部品に転じると、最終製品の信頼は、製品を構成する部品全体の信頼によって成り立つことを示している。サプライチェーン全体の信頼を構築するということは、サプライチェーン全体で、最終製品を構成する部品や製品の

全体の信頼の根拠となる証拠を保持することに他ならない。

従来は、最終製品の信頼を確認するとしても、最終製品を構成する部品や製品の信頼は暗黙的に信頼するということにとどまっていた。しかし、1.で述べたような形でサプライチェーン全体の信頼を構築すれば、最終製品を構成する部品や製品の信頼の証拠をたどることが可能になる。具体的には、図 1 を例にとれば、組織 B は、組織 A に証拠を提示するだけでなく、組織 C からの証拠の提示を受けており、これらのふたつの証拠を関連づけることが可能である。これをサプライチェーン全体に適用すれば、最終製品を構成する部品や製品の全体の証拠をたどることが可能になる。

3. 「信頼の創出」の技術プロセス

本章では、製品やサービスを授受する組織どうしが、信頼を構築するために実施する「信頼の創出」の技術プロセスを説明する。以降の説明では、提供する製品等を実現するために組織が実施する設計～調達～製造・検査～流通～運用～保守に係る業務プロセスを、「価値創造プロセス(VCP: Value Creation Process)」[2]と呼ぶ。

「信頼の創出」は、次の(1)～(4)のステップにより実現される。各ステップを、図 3 に従い説明する。

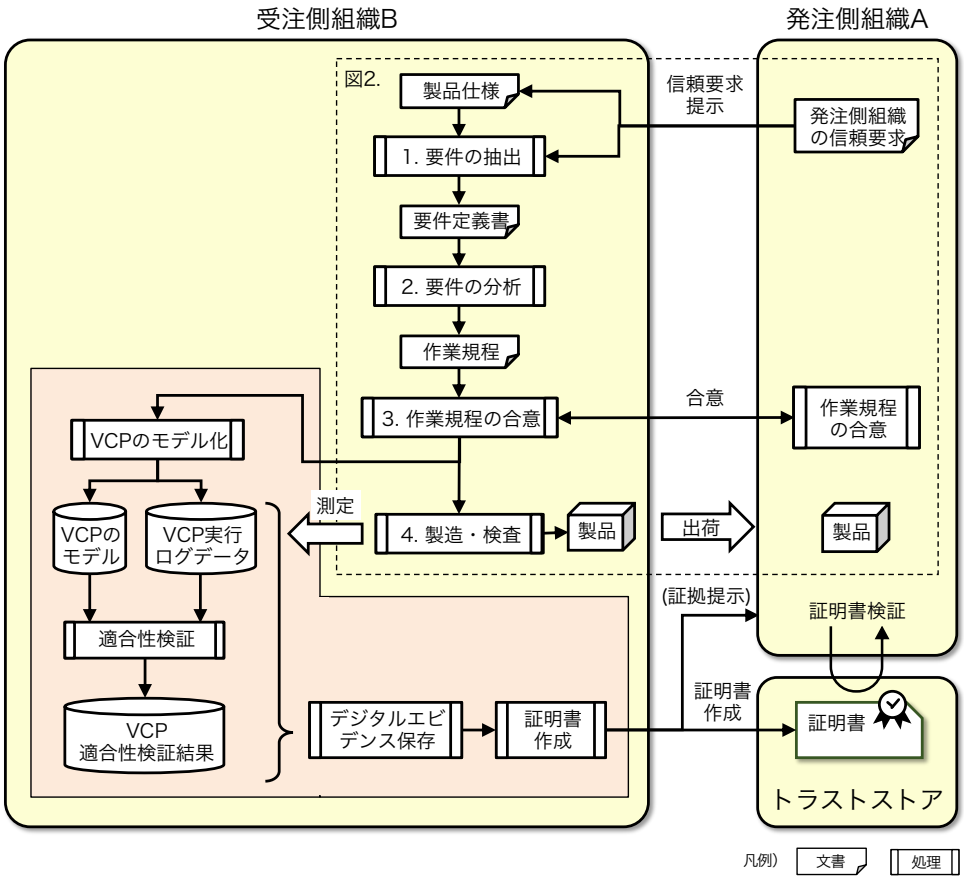

図 3「信頼の創出」の技術プロセス

(1) VCP のモデル化： 正しい VCP を設計し、「VCP のモデル」を作成する。

・受注側組織 B は、要件定義書に含まれる信頼要件を分析して、「VCP のモデル」を作成する。VCP のモデルは、信頼に関する要求を満たす製品を製造する正しい作業手順を、プロセスモデル記述言語を用いて記述したモデルである。VCP のモデルは、フィジカル空間の業務(VCP)が正しく実施されているか否かを、サイバー空間上の IT システムで検証するための規範モデルである。

・VCP のモデルは、対象業務を実施者（ヒト、ソシキ）、原材料（モノ）、業務基準（データ）、業務手順（プロシージャ）、業務設備（システム）の 6 つの視点で分析して作成する。業務とは、ソシキやヒトが、業務手順であるプロシージャに則り、モノやデータを含むシステムを使って、製品やサービスの実現を図る営みだからである[2]。

・ヒトやモノが業務を適正に実行していることの証拠データの決定については、2.2 で述べた。さらに受注側組織は、証拠データの測定方法も決めなければならない。例えば、業務プロセスにおけるヒトの行動については、業務現場をビデオ撮影して、そのデータを採取する方法が考えられる。また、使用する工具等のモノが規程に則って使われているか否かは、モノの IoT デバイス機能でデータ測定（例：トルクレンチの締め付け強度データ）して、判定することが可能である。

(2) VCP の適合性検証： 受注側組織は、以下のように、自己の VCP の実行状況が、「VCP のモデル」に適合しているか否かを検証する。

・製造現場で証拠データを測定し、「VCP 実行ログデータ」として蓄積する。VCP 実行ログデータは、VCP が規程どおりに実行されているかを検証するための基礎データである。

・VCP 実行ログデータを、(1)の VCP のモデルと照合して、VCP の実施状況が VCP のモデルに適合しているか否かを検証する。この結果を「VCP 適合性検証結果」と呼ぶ。

(3) デジタルエビデンスの保存： 受注側組織は、以下のように、VCP 適合性検証結果を用いて証拠を作成する。

・(2)の適合性検証に用いた VCP のモデルと VCP 実行ログデータ、VCP 適合性検証結果を用いて、VCP の適合性検証を行った証拠である「デジタルエビデンス」を作成する。

・一般的に受注側組織は、デジタルエビデンスを第三者に開示しない。ただし、信頼に関わる事故に起因する係争等が発生した場合には、然るべき機関等の第三者からの要求に応じてデジタルエビデンスが開示され、実行業務の適合性の証拠として活用されることも想定する。

(4) 「証明書」の作成：デジタルエビデンスを用いて標準形式の「証明書」を作成する。

・受注側組織は、図 3 に示すとおり、VCP の「デジタルエビデンス」を用いて標準形式の「証明書」を作成する。作成した証明書は、SC に参加する組織が権限に応じて読み書きが可能な証明書の貯蔵庫（トラストストア）に格納する。最後に受注側組織は、発注側組織の信頼要求に適合した業務の実行の証拠として、証明書を提示する。発注側組織は、証明書を検証して、納入された製品等が自己の信頼要求に適合しているか否かを検証することができる。発注側組織による「証明書検証」により、「発注側組織の信頼要求」の提示から始まった「組織間の信頼」の形成のサイクルが完了する。

・信頼性を備えた証明書を作成する組織的な仕組みとして、2 通りが考えられる。図 3 に示したのは、受注側組織が証明書を作成する方法である。この方法では、受注側組織が 3 章「信頼の創出の技術プロセス」に示した通りに VCP の適合性を検証するシステムを構築していることを、発注側組織が事前に認めておくことが、信頼の前提として必要となる。この前提の下で、発注側組織は、受注側組織が作成する証明書を信頼して、製品等の適合性を検証する。この方法は、受注側組織が、自己の製品等の適合性を「第一者認証」する仕組みである。

・信頼性を備えた証明書を作成する別の組織的な仕組みとして、信頼できる第三者機関（TTP: Trusted Third Party）（図 3 及び図 4 には示さない）が証明書を作成する方法がある。この場合、上述の受注側組織に対する信頼の前提を、TTP に対する信頼の前提へと置き換える必要がある。この前提の下で、発注側組織は、TTP が生成する証明書を信頼して、製品等の適合性を検証可能となる。この方法は、TTP が、受注側組織の製品等の信頼性を「第三者認証」する仕組みである。TTP は、「デジタルエビデンス」を用いて適合性検証を実施し、証明書を作成する。そのため、受注側組織は、「デジタルエビデンス」を TTP に開示する必要がある。

4. 「信頼チェーンの構築」の技術プロセス

本章では、SC に参加する各組織が、SC 全体を通しての製品やサービスの信頼を形成するために実施する「信頼チェーンの構築」の技術プロセスを説明する。「信頼チェーンの構築」は、次の(1)～(2)のステップにより実現される。各ステップを、図 4 に従い説明する。

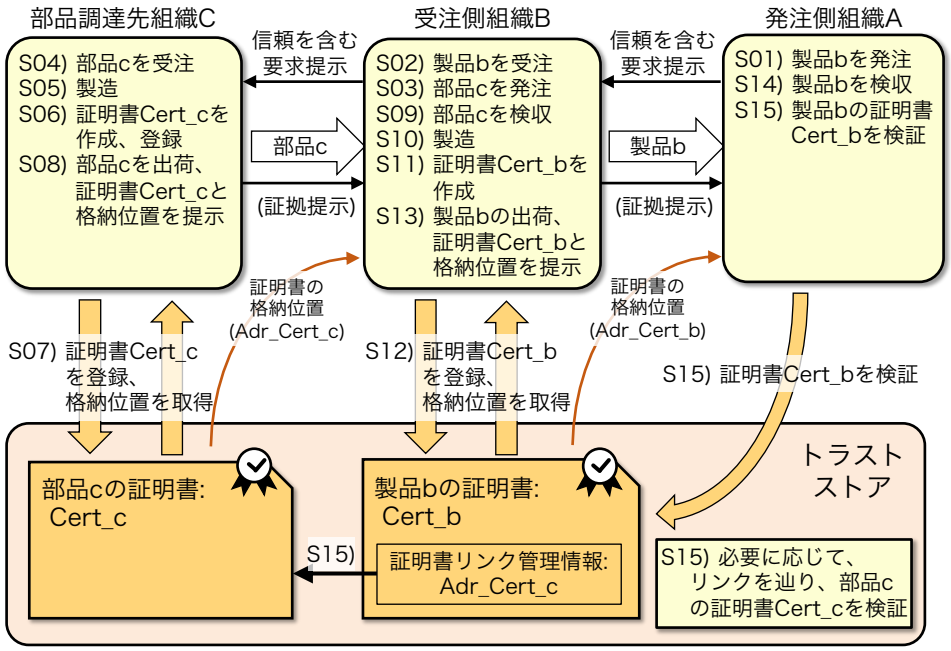

図 4「信頼チェーンの構築」の技術プロセス

(1) 証明書間のチェイニング: SC の信頼の繋がりを、証明書の繋がりに関係づける。

・1 組の受発注に関わる組織間の信頼だけでは、SC 全体の信頼は構築できない。このためには、2.3 に述べた信頼チェーンの構築が必要である。以下では、図 4 に従い、証明書の繋がりを管理する仕組みを説明する。図 4 は、発注側組織 A、受注側組織 B および部品調達先組織 C の 3 者間の証明書の繋がりを作成する流れを、S01～S15 の順序で示している。

・受注側組織 B は、作成した証明書 Cert_b をトラストストアに格納し(S12)、発注側組織 A に提示する(S13)。トラストストアは、SC に参加する組織が、各自の権限に応じて読み書きが可能な証明書の貯蔵庫である。受注側組織 B は、証拠の提示の際に、証明書のトラストストア内の格納位置 Adr_Cert_b を、発注側組織 A に提示する。SC に参加する全ての受注側組織は、証明書をトラストストアへ格納し、証明書の格納位置を発注側組織へ提示するものとする。

・受注側組織 B は、自社製品 b の証明書 Cert_b を作成(S11)するときに、使用した部品 c の証明書 Cert_c の格納位置 Adr_Cert_c を、証明書リンク管理情報として証明書 Cert_b に格納する。この処理によって、SC 上の組織 B と組織 C との信頼の繋がりが、トラストストア内の証明書 Cert_b と Cert_c の繋がりとして表現される。なお受注側組織 B は、部品 c を検収した(S09)ときに、部品調達先組織 C から格納位置 Adr_Cert_c を提示されているため、上記の証明書 Cert_b への格納が可能である。

(2) 信頼のチェーンの検証: 発注側組織は、製品の証明書を検証する。

・上記説明した証明書を繋げる仕組みにより、製品の SC 全体に渡って、製造に参加した組織が、それぞれ信頼の要求に適合した製造を実施したか否かを、発注側組織が検証することが可能となる。

・この仕組みによれば、SC の最終的な製品またはサービスに対する信頼の検証だけでなく、SC の製造の途中の段階でも、中間部品等に対する信頼の検証が可能となる。

なお、3 と 4 で記述した内容は、受注生産品であるか否かに関わらず、汎用的に適用可能であることに注意されたい。

5. 信頼構築技術の効果と課題

本信頼構築技術について、実際の事故事例に適用した場合の効果と課題を説明する。第 1 報で紹介した事故事例のうち 6 例について、表 1 に事故内容と特徴を示す。

表 1 信頼を毀損する事故事例

No	事例名	内容	規定との関係	実行主体	不正/過失
1	航空機副操縦士の乗務前過剰飲酒[3]	酒酔いの操縦士が、アルコール検査をすり抜けて航空機を運行	違反	従業員単独	不正
2	産業用ゴム製品の検査不正[4]	検査員が、怠慢を理由に検査業務を一部実行せず	違反	従業員単独	不正

3	ネットワーク・ルータへのバックドアツールの搭載疑惑[5]	業務委託先の運送会社による運送中に、第三者が製品を開封して、不正ツールをインストール	違反	第三者	不正（攻撃）
4	「ハラール認証製品」のハラール不適合問題[6]	製造プロセス設計時の検討が不十分であったために、ハラール不適合品を製造	不備	自社組織	過失
5	ディーゼル車の排気ガス不正[7]	車両製造者が、不正な設計・製造・検査業務を組織的に実施し、不良車両を製造	違反	自社組織	不正
6	サーバ・マザーボードへの情報漏洩チップの組込み疑惑[8]	業務委託先の基盤製造者が、情報漏洩チップ付きの不正基盤を組織的に製造	違反	委託先組織	不正（攻撃）

5.1. 信頼構築技術の効果

表 1 の項番 1, 2 は、規程違反による事故事例である。事故原因の作り込みは、企業の単独の従業員によるものであり、意図的な不正行為である。これらの事例では、業務手順の管理規程として規定すべき内容は単純明白であり、我々の信頼構築技術は非常に有効な対策である。企業は、技術的手段と業務プロセスの改善を組み合わせることで、本事例の不正を防止できる。具体的には、項番 1 の場合は、アルコール検知器等の技術的手段と、搭乗点呼業務プロセスの改善の組合せにより、飲酒者によるアルコール検査の不正なすり抜けを防止する。項番 2 の場合は、監視カメラや検査機器モニタリング等の技術的手段と、検査業務プロセスの改善の組合せにより、検査員による検査業務の意図的な怠慢を防止する。

項番 3 は、業務委託先の運送事業者の運送中に、第三者が製品梱包を開封して、不正ツールをインストールしたとされる事例である。この事例は、第三者による意図的攻撃であり、業務プロセスの脆弱性を突いた例である。この攻撃事例に対して、我々の信頼構築技術は、有効な対策である。業務委託元の製造事業者は、委託先の運送事業者に対して、運送業務プロセスに監視カメラや梱包開封防止装置等の技術的手段を組み込んで、第三者による製品への不正アクセスによる攻撃を防止するように要求することが考えられる。業委託先の事業者は、委託業務の適正な実施を示す証明書を業務委託元に提示し、委託元は証明書を検証することで、流通時の不正行為の有無を検証できる。

以上をまとめると、本信頼構築技術は、不正の防止に対して、一定の効果があると言える。

5.2. 信頼構築技術の課題

表 1 の項番 4 は、5.1 に示した規定違反の事例とは異なり、事故原因が規程の不備によるものである。事故原因の作り込みは、規程を作成した組織によるものであり、業務手順の分析漏れあるいは分析誤りという過失行為である。本事例は、ハラール認証の理解が容易でないために、製造工程や業務規程に漏れが起きて、ハラール認証に適合しない製品を製造したと考えられる。この食品製造者は、製造業務

プロセスを精査し、技術的手段を組み合わせることで、ハラール認証に適合する製造工程の実現を試みたに違いない。一般に、認証の要求事項の理解が十分でないと、正しい業務プロセスの作成は困難となる。そして、VCP の適合性を検証するシステムを正しく構築することもまた、困難となるだろう。

項番 5 は、項番 1 から 4 の事例と異なり、事故原因の作り込みが、企業による組織的不正である。こうした組織ぐるみの意図的な不正行為は、組織自体による阻止が望めない。我々の信頼構築技術も、意図的に不正な証拠を生成するように使われれば、不正への有効な対策とはなり得ない。本件のような組織的な不正に対しては、権威ある第三者機関が、製品の法的規制への適合性検証の検査業務を厳格に実施することでしか、不正は阻止できないだろう。

項番 6 では、事故原因の作り込みが、業務委託先の製造事業者による組織的かつ意図的な不正である。項番 5 と同様に、こうした組織ぐるみの意図的な不正行為は、その組織自体による阻止は望めない。従って、我々の信頼構築技術も、本事例の不正への有効な対策とはなり得ない。

まとめると、VCP の適合性を検証するシステムは、それを構築する組織の知見を超えては構築できないし、事実と異なる証拠を意図的に組み込もうとする不正への対抗は容易ではない。そのような適用限界があることは、今後の課題である。

6. 信頼に対する従来の考え方との関係

信頼構築技術は、サプライチェーンにおける信頼を構築するための技術である。「信頼」に対応する英語は、”trust” と “trustworthiness” がある。後者の方が前者より広い概念であり、ここで論じている「信頼」は後者に近い。 “trustworthiness” は、IT の分野でも 20 年以上前から考えられてきた。

[引例 1] National Research Council. “Trust in Cyberspace”. 1999.[9]

The degree of confidence one has that the system performs as expected in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks.

また、近年の IoT 関連の業界団体では、trustworthiness を以下のように定義している。

[引例 2] Industrial Internet Consortium. “Vocabulary”. V2.1, August 2018.[10]

Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks.

2 つの引例に共通する中心的な記述は、「システムが期待通りに動作することに対する、根拠あるいは証拠に基づいた確信の度合い」である。これは、「図 1 信頼構築の基本的考え方」とほぼ同じ内容である。

図 1 は、「発注側組織の要求通りにシステムが動作することについて、受注側組織側組織がその証拠

を発注側組織側組織に提示する」ことで、「発注側組織側組織の信頼を構築」する図式である。この図式で、「要求」を「期待」に置き換え、「証拠提示」を「根拠あるいは証拠」に置き換えると、「信頼の構築」の図式は、2 つの引例のいう「確信の度合い」を高める図式と見なすことができる。

[引例 3] NIST. “Framework for Cyber-Physical Systems”. Release 1.0., May 2016.[11]

Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but not limited to, safety, security, privacy, reliability and resilience.

本引例については、「要求」を ”design (requirements)” と考え、「証拠提示」を ”demonstrable likelihood that the system performs” と考えることで、「信頼の構築」の図式と変わらない。

以上に示したとおり、本報告の信頼構築の考え方は、”trustworthiness” に関わる従来の考え方と、ほぼ同じであることがわかる。

7. まとめ

最後に、信頼構築技術がどのような付加価値を生み出し、サイバーフィジカル時代にどのように貢献できるかを述べる。

信頼構築技術には、サプライチェーンの信頼確立に加えて、業務プロセス全体を効率化し、低コスト化する付加価値をもたらすことが期待される。冒頭に述べたとおり、現代のサプライチェーンは複雑化とグローバル化の一途をたどっている。実世界の製造あるいは運用業務を、サイバーフィジカルシステムにより管理することで、第一に製造現場の業務管理コストの低減が可能となる。さらに、万一製品やサービスの信頼を毀損する事故が発生した場合にも、事故原因の迅速な究明や、対策立案の容易化により、生産プロセスのダウンタイムを最小化し、事故対応コストを最小化することが可能となる。

信頼構築技術がもたらすサイバーフィジカル時代への究極的な貢献とは、人に優しく暮らしやすい世界の実現である。信頼構築技術は、製品やサービスへの「信頼」を確立する。前述の Industrial Internet Consortium(IIC)は、「信頼」を「環境障害、人為的エラー、システム障害、攻撃が起きた場合にも、安全性、セキュリティ、プライバシー、信頼性、回復力という 5 つの特性に関して、システムが期待どおりに機能する確かさの度合い」と定義している。我々の生活を支える製品やサービスが、上記 IIC があげる様々な障害や攻撃に直面したとしても、5 つの特性に関して期待される振る舞いを保ち続けることは、人に優しく暮らしやすい世界を実現する上での大きな支えとなるに違いない。

8. 謝辞

本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されています。

参考文献

[1] 国立研究開発法人産業技術総合研究所. “サプライチェーンにおける信頼構築に向けて”. 2019.10
https://www.cpsec.aist.go.jp/achievements/CPSEC-WP-2019001.pdf

[2] 経済産業省. “サイバー・フィジカル・セキュリティ対策フレームワーク”. Ver1.0, 2019.4
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

[3] BBC NEWS JAPAN. “JAL、英で実刑判決の副操縦士を懲戒解雇　乗務前に過剰飲酒”. 2018.11.30
https://www.bbc.com/japanese/46395567

[4] TOYO TIRE 株式会社. “産業用ゴム製品（シートリング）問題に関わる原因究明及び再発防止策について”. 2017.3.24
https://www.toyotires.co.jp/uploads/2017/03/20170324.pdf

[5] ITmedia News. “NSA は輸出する Cisco 製品にバックドアツールを仕込んでいた ── スノーデン氏関連の新刊書が暴露”. 2011.5.15
https://www.itmedia.co.jp/news/articles/1405/15/news096.html

[6] 味の素株式会社. “インドネシアにおけるハラール問題について”. 2001.1.6
https://www.ajinomoto.com/jp/presscenter/press/detail/2001_01_06.html

[7] United States Environmental Protection Agency. “Notice of Violation”. 2015.9.15
https://www.epa.gov/sites/production/files/2015-10/documents/vw-nov-caa-09-18-15.pdf

[8] Bloomberg Business week. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”. 2018.10.4
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[9] National Research Council. “Trust in Cyberspace”. The National Academies Press, 1999.

[10] Industrial Internet Consortium. “The Industrial Internet of Things Volume G8: Vocabulary”. V2.1, August 2018.
https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf

[11] NIST. “Framework for Cyber-Physical Systems”. Release 1.0, May 2016.