CPSEC-WP-20200003

サプライチェーンにおける信頼構築に向けて
－ 第 3 報　信頼構築技術がもたらすサプライチェーンの姿と相互運用性の確保　－

2020 年 10 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が数多く報告されている。ホワイトペーパー第 1 報では、それらの事故分析から、規程順守が信頼の鍵であることがわかり、信頼の構築に向けた基本的な考え方を示した。ホワイトペーパー第 2 報では、発注に際して明示する信頼に関する要求、それを満たすことの受注側組織による証拠であるデジタルエビデンス、デジタルエビデンスから生成される証明書、証明書の連鎖で構成される、サプライチェーン全体の信頼を構築する技術（信頼構築技術）を説明した。第 3 報では、先ず、信頼構築技術が普及した場合のサプライチェーンの姿を概観する。そのような状況になるためには、相互運用性の確保が必要になる。どのような相互運用性が必要になるのか、そのためのステップも含め、検討する。

1.　信頼構築技術が変えるサプライチェーンの姿

第 1 報及び第 2 報に記述したとおり、信頼構築技術を使ったサプライチェーンは、発注時には機能だけでなく信頼に関する要求も含めた要求（以下、信頼要求と呼ぶ）を提示し、製品やサービスの納品時には併せて製品やサービスの信頼を判断する根拠となる証明書が提供され、必要であれば証拠も提供される。証明書は、併せて、トラストストアにも格納される。

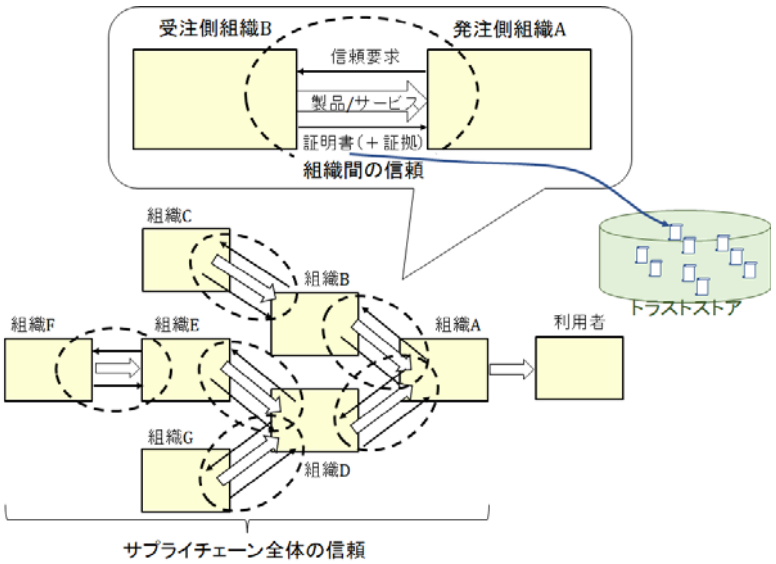

図 1　信頼構築技術がつなぐサプライチェーン

信頼構築技術が普及すれば、信頼を重視するサプライチェーンにおいては、全ての製品やサービスの受発注において、信頼要求と証明書が授受されるようになるだろう。
そうなると、信頼要求と証明書は、信頼を重視する組織においては、受発注のコミュニケーションツールになる。すなわち、

- 受注側組織は、信頼要求を見れば、自組織の製品やサービスが信頼要求に適応できるかを判断できる。
- 発注側組織及び利用者は、証明書を見れば、製品やサービスが信頼要求を満たすかを判断できる。

これらは、信頼を重視するサプライチェーンにおいて、発注先決定の自由度を上げることにつながる。
発注側組織及び利用者は、例えば e マーケットプレイスに信頼要求を提示したり、トラストストアに格納された証明書を検索したりすることで、自組織が要求する信頼の条件を満たす製品やサービスを提供する組織をより広く知ることができる。一般にサプライチェーンの受発注関係は一昔前の固定的な関係から再編されつつあるが、コストの観点からの発注先変更が多かったであろう。しかし、サプライチェーンにおける部品等の発注において重要なのはコストだけではなく、信頼も重要な要因である。信頼要求も証明書も受発注関係における信頼を可視化する効果があり、その結果として、信頼を重視する場合の発注先決定の自由度を上げる。
信頼を重視する受注側組織にとって、信頼構築技術は、上記とは逆に、信頼に対する自組織の取組みを発信して選択される幅を広げるツールになる。すなわち、受注した製品やサービスを納品する際には併せて証明書をトラストストアへ格納するから、トラストストアの参照権限のある組織全てに、証明書を見てもらうことができるようになる。従来、製品やサービスの信頼性は、目に見えず、実際に使ってみて初めて判断できた。経験に基づく判断は重要であるが、組織の製品やサービスに対する信頼を可視化する要素のひとつである証明書は、客観的な信頼性の尺度を与えることになる。トラストストアの存在は、信頼性をオープンな尺度にするものでもある。従来経験によって得られた製品やサービスの信頼性の情報は、人を介して伝達されて来たであろう。よって、その伝達は局所的であった。トラストストアを参照できれば、世界のどこからでも、信頼できる製品やサービスの存在を知ることができる。信頼に足る製品やサービスは、トラストストアの存在によって、その組織の規模によらず、市場を世界に広げる可能性がある。
信頼要求と証明書による信頼の可視化によって、信頼が製品やサービスの選択基準としてより重視されることになるであろう。製品やサービスの価格が重視されるのは、それらを購入する組織においては、価格が収支に直結するからであるだけでなく、価格が数値というひとつの基準で容易に比較可能だからである。信頼が組織にとって重要であることは、疑う余地はない。しかし、従来、信頼を評価項目にしようとしても、妥当なものさしがなかった。信頼要求と証明書は、数値ほど単純ではないが、信頼の比較の部分解を与えるものである。このような尺度が与えられれば、信頼は評価項目として使い易くなり、重視されることになる。選択基準として重視されるようになれば、組織も信頼性向上により積極的に取り組むことになるであろう。その結果として、社会全体において、製品やサービスの信頼性が向上し、安全や安心して生活できる社会が実現されるであろう。信頼構築技術は、そのような形で、社会に貢献し得る技術である。

証明書発行を支えるのは、第 2 報に述べたように、価値創造プロセス（Value Creation Process（VCP））におけるデジタルエビデンスの生成と保存である。製品やサービスの製造プロセスに関わるデジタルエビデンスが生成され保存されることは、信頼性向上の契機を与えるものである。信頼構築技術は、副次的にも、社会の信頼性向上に寄与する技術である。
信頼要求と証明書は受発注組織間のコミュニケーションツールになる、と述べた。しかし、そうなるためには、サプライチェーンにおいて、相互運用可能でなければならない（相互運用できなければ、コミュニケーションは成立しない）。サプライチェーンにおいては、一組の受発注においても、業界をまたがる場合がある。よって、上記の相互運用性は、業界を超えて実現されるべきである。どのような相互運用性が実現されなければならないかを、次に考える。

2. 信頼構築技術の相互運用性のための枠組み

相互運用性が最も重要なのは、信頼要求と証明書である。しかし、それを実現するためには、それらを包含する枠組みが必要である。その枠組みを信頼構築フレームワークと呼ぶことにする。ここでは、信頼構築フレームワークの概要を示す。

2.1. 信頼構築フレームワーク

信頼構築フレームワークの説明の前に、第 2 報で述べた信頼構築技術を復習する。
信頼構築技術は、製品やサービスが提供する価値が確実に提供されるために、製品やサービスの製造プロセスである VCP に対して、規程を含む VCP のモデルである機械可読な VCP モデルを作成し、VCP が VCP モデルに照らして正しく実施されているか検証しつつ、デジタルエビデンスを生成して、最終的に証明書を生成する技術である。その中心は、規程が正しく実施されたかを検証して製造を実施することである。
世の中には、規程を正しく実施したかを検証する枠組みは、提案されていない。しかし、対象が、規程ではなく製品自体であれば、セキュリティ評価認証の枠組みであるコモンクライテリア（Common Criteria（CC））が存在する。CC は、製品のセキュリティ評価を実施するための種々の道具が揃っている。すなわち、セキュリティ機能要件のカタログ、セキュリティ機能が確実に実装されたかを確認するため要件であるセキュリティ保証要件カタログがあり、製品の要求定義書（セキュリティターゲット（Security Target（ST））と呼ばれる）はこれらのカタログから要件を抽出して作成する。また、製品毎に ST があってもそれらの比較は難しいので、製品分野に共通の要求定義書（プロテクションプロファイル（Protection Profile（PP）と呼ばれる）を定義して、ST を PP に準拠して作成するという方法も用意している。製品は、ST を基に CC の評価方法である共通評価方法（Common Evaluation Methodology（CEM））に基づいて評価認証され、認証書が発行される。PP に準拠して ST を作成した製品は、その PP 準拠であることが認証書に明記される。信頼構築フレームワークは、CC の体系を参考にする。信頼構築フレームワークは、CC の評価対象である製品のセキュリティ機能を、製品の製造等の規程に置き換えたものと言うことができる。

2.2. 信頼性クライテリア

信頼性クライテリアは、CC における CC 自体に相当する。製品やサービスの提供において、信頼性のための規程を順守していることを、すなわち信頼性を客観的に評価し認証するための評価基準

である。信頼性クライテリアが示すべきことは、組織のプロセスが規程を順守していることである。CC に照らして考えれば、機能要件に相当するのが規程であり、保証要件に相当するのは規程の順守の示し方である。CC に倣って、それぞれを信頼性機能要件・信頼性保証要件と呼ぶことにする。信頼性保証要件では、エビデンスのあり方・生成・管理方法が規定され、保証の厳密さによって、いくつかの段階が規定される。
製品やサービスがこれらの要件を満足するかを評価するための信頼性評価方法も必要であり、これについては 2.4 で述べる。

2.3. 信頼性個別要件

信頼性個別要件は、CC の ST に相当する。製品やサービスに対して、受注側組織の状況や環境に即して、設計～調達～製造・検査～流通～運用～保守のプロセスに関わる信頼性機能要件群及び信頼性保証要件群を定義した文書である。名前のとおり、信頼性個別要件は、個別の製品やサービスに対して、定義された要件集である。よって、信頼性個別要件は、製品やサービスの数だけある。
上記のとおり、ある製品やサービスが満たすべき信頼性機能要件の全体は、その製品やサービスの価値を実現するための規程である。規程を構成する各項が、個々の信頼性機能要件になる。組織内の規程は、組織に蓄積された営業秘密だから、開示されない。しかし、信頼性機能要件は、共有されるものであり、営業秘密にならない程度に、しかも、信頼性に対してなすことがわかる程度に抽象化されたものである。

2.4. 信頼性評価方法

信頼性評価方法は、CC の CEM に相当する。製品やサービスの提供のための規程順守の評価手順、評価機能、第三者機関による確認・監査の枠組みを定める。エビデンスに基づく信頼性保証要件の確認方法などを含む。

2.5. 信頼性共通要件

信頼性共通要件は、CC の PP に相当する。製品や業界、地域や国家の相違を吸収し、製品や業界、地域や国家をまたがって、信頼性基準を共有可能な信頼性機能要件群及び信頼性保証要件群として表現したものである。信頼性共通要件を基に、業界や製品、地域や国家の状況に応じて、信頼性個別要件を定義することができる。
以上の信頼構築フレームワークの信頼性クライテリア等と信頼要求や証明書との関係を、以下に図示する。

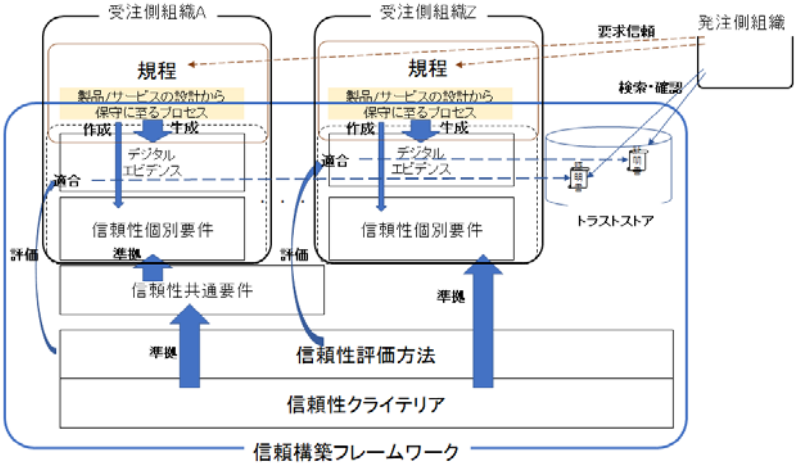

図 2　信頼構築フレームワークの概要

同一の信頼性共通要件から作られた信頼性個別要件を持つ製品やサービス同士は、信頼性機能要件群及び信頼性保証要件群が共通しているので、すなわち、規程順守の要件が共通しているので、同等に信頼できると考えることができる。

CC における PP は、例えば、IC カード、ファイアウォールなど、製品分野毎に作られるプロファイルである。PP は製品のセキュリティ機能の要件を含むから、製品分野が異なれば、異なる PP が必要になる。これに対して、信頼性共通要件は、規程順守の要件集である。製品分野が異なっても、組織の製造等に関する規程には共通性があるので、信頼性共通要件は業界を超えて適用できる場合もある。すわなち、信頼性共通要件は CC の PP よりも広い適用分野を持ち得る。

CC における PP が業界団体で作成されるのと同様に、信頼性共通要件も、当該分野の製品やサービスの製造に詳しい業界団体で作成されることになるであろう。ひとつの業界で作成されれば、上述のとおり、信頼性共通要件は、製品やサービスの分野を超えて再利用されることが期待できる。このようにして作成された新しい信頼性共通要件が、再利用範囲を拡大するかも知れない。また、再利用範囲の外側で、別の信頼性共通要件が作成されるかも知れない（図 3）。

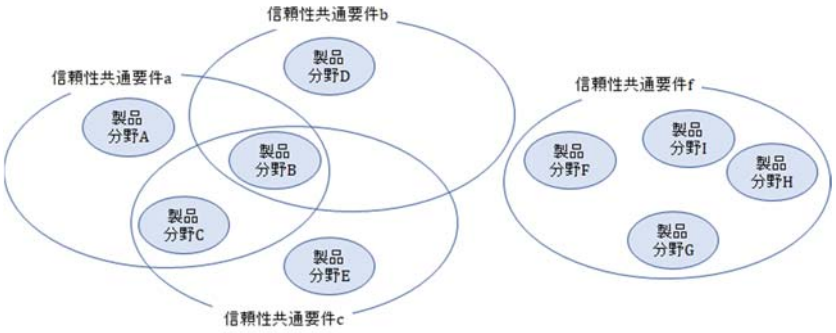

図 3　製品分野と信頼性共通要件の関係（模式図）

2.6.　信頼性クライテリアの標準化

既に述べたように、信頼性機能要件は、営業秘密を含まないように抽象化した規程の要素である。

抽象化した規程の要素である信頼性機能要件を蓄積することによって、信頼性個別要件は作成可能になる。
規程の抽象化によって、信頼性個別要件は他の組織や事業分野で再利用されるかも知れない。そうなれば、その信頼性個別要件は、信頼性共通要件と考えることもできる。そのようにして信頼性共通要件ができれば、それから派生して新たな信頼性共通要件が作られることもあるだろう。
抽象化された信頼性機能要件が蓄積されれば、CC パート 2 と同様に、信頼性機能要件カタログである信頼性クライテリアパート 2 が構成されることになるだろう。規程は、製品やサービスの機能ほどは事業分野によって異ならないが、それでも事業分野に依存する。事業分野または事業分野群の信頼性クライテリアパート 2 が出来て、それが更に蓄積され抽象化されて、事業分野に依存しない最終的な信頼性クライテリアパート 2 ができることになるだろう。
信頼性個別要件における信頼性機能要件は、抽象化された規程である。その抽象化された規程が順守されていることの示し方が信頼性保証要件である。その示し方の厳密さに応じて、デジタルエビデンスや証明書の内容が決まる。この厳密さは、CC における EAL（Evaluation Assurance Level）と同様にレベル分けが成されると使い易くなるであろう。これらを体系的にまとめて、CC パート 3 と同様に、信頼性保証要件カタログである信頼性クライテリアパート 3 が構成されることになるだろう。

3. 信頼要求の標準化

信頼性共通要件は、製品やサービスの分野に対する信頼性機能要件群及び信頼性保証要件群であり、規程順守のための要件集である。また、2.5 に述べたように、信頼性共通要件は業界を超えて適用できる場合があるので、受注側組織だけでなく、発注側組織にとっても、理解可能な文書である。よって、信頼性共通要件は、製品やサービスの発注に当たり、製品やサービスの信頼要求に使うのに適切である。
信頼要求に信頼性共通要件を使う場合、文書としての信頼性共通要件をその度毎に提示する必要はない。信頼性共通要件は予め公開されるものであるから、信頼性共通要件に識別情報を与え、その識別情報を提示すれば十分である。信頼性共通要件の作成すなわち標準化は、業界団体でなされるべきであろうことは既に述べた。信頼性共通要件の識別情報の標準化についても、同様であろう。識別情報の形式は機械可読であればどのようなものでも特に問題はないが、識別情報の利用が広がって行った場合でも衝突が起こらないようにしておくべきである。そのためには、識別情報が一意になるようにするための登録機関が必要である。識別情報と併せて、国際標準化が必要かも知れない。
第 2 報で述べたように、信頼要求は、機能だけでなく信頼に関する要求も含めた発注時の要求である。信頼に関する要求については、上記のとおり、信頼性共通要件及びその識別情報を標準化すれば良い。その他の機能等の要求については、本書の範囲を超えるが、少し考察してみよう。
信頼要求は、発注側組織と受注側組織で交換される情報である。多くの場合、ひとつの組織に対して、発注側組織はひとつではないし、受注側組織もひとつではない。すなわち、一般的には、製品の発注と受注の関係は多対多の関係にある。信頼要求の形式がそれぞれ異なっているとすれば、受注側組織は発注側組織の数だけの信頼要求の処理方法が必要になる。これは、双方の組織にとって、大きな負担になる。できる限り関係する業界で共通化されることが望ましい。

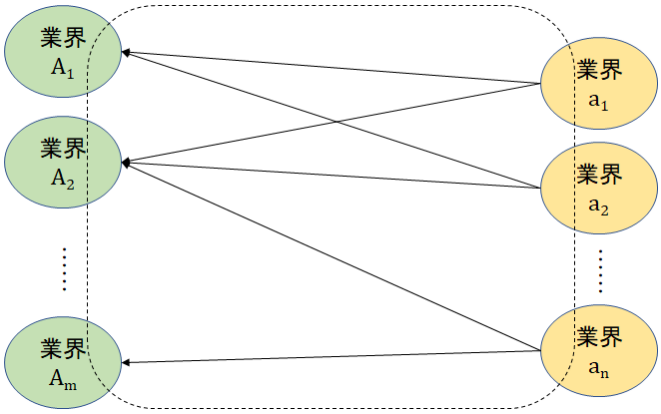

図 4 業界をまたがる信頼要求の授受

図 4 の業界 a_1 から出るふたつの矢印は、業界 a_1 に属する発注側組織が業界 A_1 と業界 A_2 の組織に発注することを表している。この場合、業界 a_1、業界 A_1、業界 A_2 では、信頼要求の形式は共通化されることが望ましい。矢印で結ばれた業界同士が同様の意味を持つとすると、業界 A_1 と業界 A_2 は業界 a_2 との間で、また業界 A_2 は業界 a_n との間で、更に業界 a_n は業界 A_m との間で、それぞれ信頼要求を交換するので、これらの業界間では信頼要求の形式は共通化されることが望ましい。このようにして関連する業界を洗い出していけば、信頼要求の形式を共通化すべき業界の範囲が決まる。

業界 A_1 の組織は、業界 a_1 の組織から発注した製品を製造するために、発注側組織になる場合がある（部品になる製品を別の組織に発注する）。図 4 の場合と同様に考えると、業界 A_1 を右側に置いた図 4 と同様の図ができ、図 4 で得たのとは別の信頼要求の形式を共通化すべき業界の範囲が決まる（ただし、図 4 で業界 A_1 が右側にも出て来ている場合は、新たな図ではなく、図 4 と同じ図になる）。上のような操作を、そこに現れる業界が参加する全てのサプライチェーンに適用すれば、共通化すべき信頼要求の形式がいくつか決まる（図 5）。これまでの操作に現れない別のサプライチェーンがあったとしても、それについては考慮する必要はない。なぜなら、その新たなサプライチェーンは、これまでの操作に現れたサプライチェーン上の組織と受発注の関係はないからである。

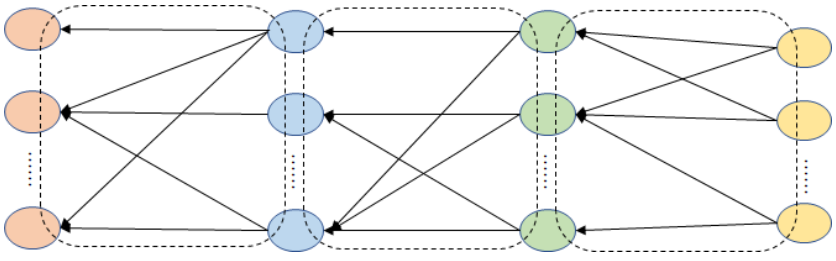

図 5 関係するサプライチェーンでの信頼要求の形式共通化

4. 証明書の標準化

証明書は、信頼要求の対になるデータである。よって、共通化されるべき業界の範囲は、信頼要求

と同様である。下流の組織は、自らが受け取る証明書だけでなく、上流の証明書を参照することもあり得る。これを考慮すると、図 5 の考察で現れる業界全体で、証明書の形式は共通化されることが望ましい。

5. デジタルエビデンスの標準化

ホワイトペーパー第 2 報にあるように、デジタルエビデンスは、原則、第三者に開示するものではない。第三者に開示されないのであれば、組織独自のものであって良いように考えられるが、完全に組織独自のものであるのは望ましくない。なぜなら、ホワイトペーパー第 2 報では、「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」としている。そうであれば、デジタルエビデンスの少なくとも一部は、必須とは言えないが、業界や関係業界に共通するものであることが望ましい。ここでは、実現に至るみちのりは長いが、デジタルエビデンス共通化の理想的な姿を考えてみる。

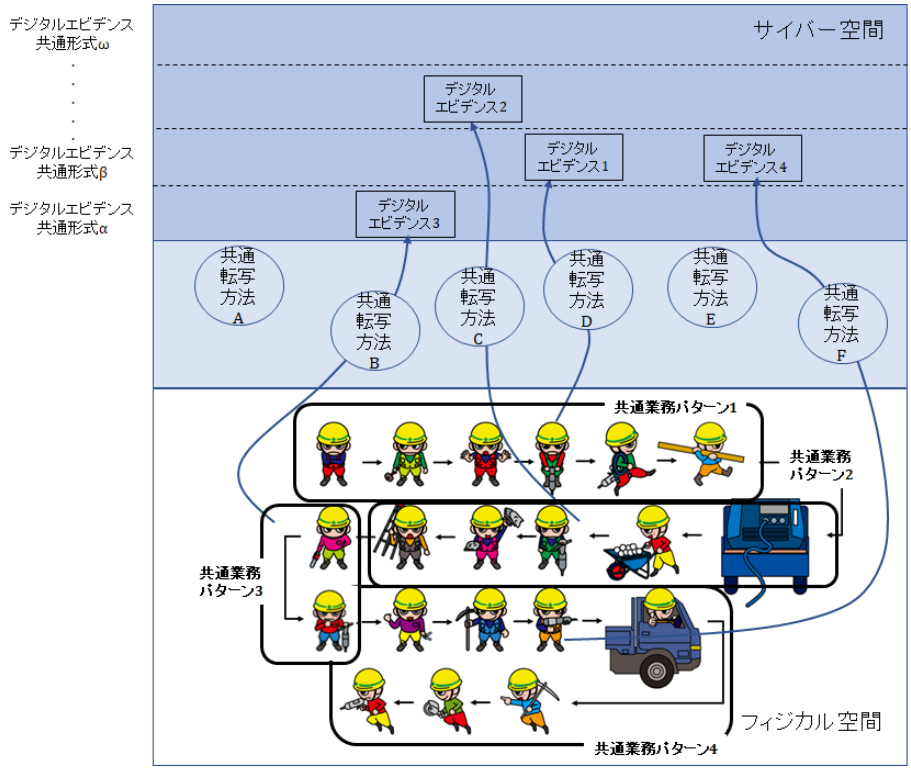

図 6 信頼構築の共通パターン化（イメージ）

デジタルエビデンスの共通化を考えると、デジタルエビデンスの元になる業務の集まり、業務の集まりからデジタルエビデンスへの転写方法（例えば、監視カメラによる画像データの取得方法等）、デジタルエビデンスの形式が、図 6 における共通業務パターン、共通転写方法、デジタルエビデンス共通形式のように、組織を超えて共通化されることが望ましい。これらが組織を超えて共通化されるためには、それ以前に各組織内での共通化が必要である。信頼性個別要件から信頼性共通要件に到達するのと同様に、組織内での共通化から組織を超えた共通化がなされるであろう。

図 6 の場合、共通業務パターン 1 に対しては、共通転写方法 D を使って、デジタルエビデンス共通形式 β でデジタルエビデンスは保存される。他に、共通業務パターン 4 も、共通転写方法 F を使って、デジタルエビデンス共通形式 β で保存される。業務内容が異なれば、追加で保存したいデータもあるだろう。その場合は、図 7 のように、デジタルエビデンス共通形式 β に拡張領域を定義することによって、共通業務パターン 1 と共通業務パターン 4 は、それぞれに追加のデジタルエビデンスを保存することができる。

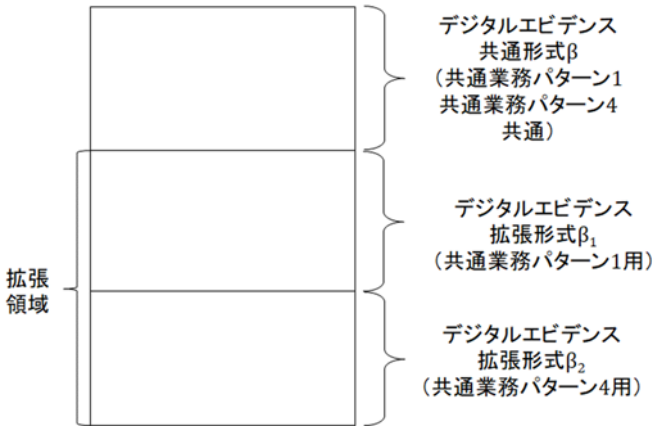

図 7 デジタルエビデンス共通形式の拡張領域（例）

ここまで信頼要求、証明書、デジタルエビデンスの 3 つについて、形式の共通化を検討した。信頼要求と証明書の共通化されることが望ましい業界の範囲は、3 に述べたとおりである。デジタルエビデンスについては、基本的には業界内で共通化されれば良いが、証明書に参照されるものについては、発注側組織が属する業界全体との間で共通化されることが望ましい。信頼要求、証明書、デジタルエビデンスのいずれにおいても、業界を越えて共通するデータ項目と業界に依存するデータ項目があるであろう。図 8 のように、それらを分類して定義することが、相互運用性のために、重要である。

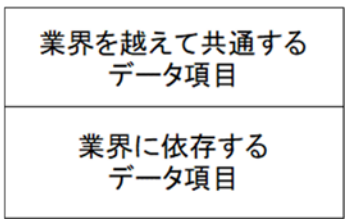

図 8 信頼要求、証明書、デジタルエビデンスにおける業界非依存共通部と業界依存部の分離

6. 国際標準化へ

以上に述べたように、各データ形式の共通化は、業界が取り組まなければ、その実現は難しい。すなわち、業界団体がデータ形式の共通化に取り組むべきである。サプライチェーンがグローバル化していることを考えれば、ひとつの国の業界団体ではなく、国際的な業界団体がデータ形式共通化に取り組むべきである。信頼要求、証明書、デジタルエビデンスのいずれも、業界団体を越えたデ

一タ形式共通化の検討が必要である。その場合は、業界団体での検討は難しく、国際標準化機構（ISO（International Organization for Standardization））や国際電気標準会議（IEC（International Electrotechnical Commission））などの国際標準化団体で検討することになるであろう。2 で述べた信頼性クライテリアについても同様である。

信頼構築技術の普及は、データ量を増大させることになる。IT の進化によって膨大な量のデータの蓄積が可能になったが、それでもデータ量の増加は抑制されるべきである。デジタルエビデンスなどのデータ量の増加も抑制されることが望ましい。信頼要求、証明書、デジタルエビデンスのうち、信頼要求は保存の必要はないかも知れないが、証明書とデジタルエビデンスは保存されることになるであろう。証明書とデジタルエビデンスは、全てが一律に保存されるわけではなく、信頼性保証要件に応じたデータ量で保存される。すなわち、信頼性保証要件が厳密でない場合は、証明書やデジタルエビデンスのサイズも削減される。

また、信頼要求に対して、それぞれの共通業務パターンから共通転写方法によってデジタルエビデンス共通形式のデジタルエビデンスを生成し、その結果として、証明書を返すプロトコルが定義されることになるであろう。このプロトコルの国際標準化によって、多様なニーズに対応する信頼構築技術を確立し、社会全体で信頼を支えることが可能になるであろう。

7. 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– 第 1 報 信頼を損なう事故事例の分析と信頼構築の基本的考え方 –”, 2019.10, https://www.cpsec.aist.go.jp/achievements/CPSEC-WP-2019001.pdf

[2] 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– 第 2 報 信頼構築技術について –”, 2020.1, https://www.cpsec.aist.go.jp/achievements/CPSEC-WP-2019002.pdf