

2021
年度

サプライチェーンのトラスト に関する課題と提言

2022年3月

JDTF サプライチェーン改革 WG

I. 内容

I. はじめに	2
II. スコープ：安心・安全に向けたサプライチェーンのトラスト	6
III. 環境状況/状況の変化	7
IV. 解決すべき課題	11
V. 解決に向けた方策.....	13
1. サプライチェーンのトラストのめざす姿	13
2. 要件.....	14
3. 実現方法	15
3-1. サプライチェーンのトラストの分類	15
3-2. 実現方法の全体像.....	15
3-3. トラストストア、デジタルエビデンス.....	16
3-4. TaaS.....	19
3-5. ベース・レジストリ	20
3-6. サプライチェーンのトラスト要件との関係	21
4. ユースケース	22
4-1. 機器から出るデータの信頼性を確保する仕組み	22
4-2. サプライチェーン全体で二酸化炭素排出量を減らす取り組み	29
4-3. 製造サプライチェーン全体のセキュリティ対策の確認	34
5. TaaS(Trust as a Service)の利用シーン・効果.....	37
VI. 提言	39
VII. おわりに	40

1. はじめに

国際社会が持続的な開発目標を目指す上での諸課題を抱えている中、日本政府は AI・5G・IoT 等のデジタル技術をあらゆる産業や社会生活に取り入れ、経済発展と社会的課題の解決を両立していく社会としての Society 5.0¹の実現を提唱している。

Society 5.0 の実現のため、様々なステークホルダが協調しデータの国際的な流通を見据えて、欧州 eIDAS 規則²など諸外国との調和を前提とした信頼性を担保する仕組みの構築に取り組むことが望まれている。日本政府は、Data Free Flow with Trust³として自由で開かれたデータ流通とデータの安心・安全の2つをポイントに取り上げている。

Society5.0 が目指す安心・安全な社会を実現するには、データはもちろん、その社会に製品やサービスを提供しているサプライチェーンにも、安心・安全が必要である。サプライチェーンとは、発注指示される一連のリソースとプロセスであり、ベンダ、製造施設、ロジスティクスプロバイダ、内部流通センタ、流通業者、卸売業者、および商品とその関連サービスの製造または提供過程、処理、取り扱い、配送または提供に関与する者が含まれる。サプライチェーンを安心・安全なものにするには、消費者に提供される製品やサービスの提供過程も含めて安心・安全にすることが必要である。

本ホワイトペーパーでは、サプライチェーンの安心・安全の確保(サプライチェーンのトラスト)に焦点をあて、その課題と提言を述べる。

¹ https://www8.cao.go.jp/cstp/society5_0/

² Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

³ 「デジタル時代の新たな I T 政策大綱」、IT 総合戦略本部、2019 年 6 月 7 日決定、<https://cio.go.jp/node/2534>

表 I-1 に参考文献と本稿で指し示すラベルを記載する。

表 I-1 参考文献

項番	作成者	文献名	ラベル
1	World Economic Forum	"Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT)ホワイトペーパー"(2021.3)	[WEF '21]
2	デジタル庁	"デジタル社会の実現に向けた重点計画"(2021.6.18)	[デジタル庁 '21]
3	Industrial Internet Consortium	"Trustworthiness"(2018.1.18) (https://www.iiconsortium.org/pdf/2017-12_4Q17_report_Trustworthiness_Final.pdf)	[IIC'18]
4	ロボット革命・産業 IoT イニシアティブ協議会 (RRI)・ドイツ Platform Industrie4.0	"IIoT Value Chain Security – The Role of Trustworthiness"(2020.9.23)	[RRI '20]
5	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 Society5.0 における新たなサプライチェーン(バリュークリエイションプロセス)の信頼性の確保に向けて Version 1.0"(2019.4.18)	[経産省'19]
6	ISO	"Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance"(2007)	[ISO 28001 '07]
7	独立行政法人日本貿易振興機構	"貿易投資相談 Q&A OEM 契約とライセンス契約の違い: 日本"(2017.8) (https://www.jetro.go.jp/world/qa/04A-011247.html)	[JETRO '17]
8	ENISA	"Understanding the increase in Supply Chain Security Attacks"(2021.7.29) (https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks)	[ENISA '21]
9	Industrial Internet Consortium	"The Industrial Internet of Things Trustworthiness Framework Foundations, Version V1.00"(2021.7.15)	[IIC '21]
10	JDTF ルール形成委員会	"デジタルトラスト協議会 ルール形成委員会, ホワイトペーパー 第1版"(2021.12.07) (https://jdtf.jp/report/rm-com)	[TaaS WP '21]
11	内閣府	"デジタル社会の実現に向けた重点計画 別紙 包括的データ戦略"(2021.6.18)	[包括的データ戦略'21]
12	環境省	グリーン・バリューチェーンプラットフォーム: サプライチェーン排出量算定をはじめの方へ (env.go.jp)より引用 (http://www.env.go.jp/earth/ondanka/supply_chain/gvc/supply_chain.html#no01)	[環境省サプライチェーン排出量算定]

表 I-2 に用語集を記載する。

表 I-2 用語集

項番	用語	英語表記	説明
1	信頼チェーン [経産省'19]	Trust Chain	信頼の創出と証明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のこと。 本書での定義；証明書のつながりで適合性を示すこと。
2	信頼チェーンの構築	Structuring Trust Chain	証明書と紐づけ情報を用いて信頼関係を連鎖させること。
3	価値創造過程 [経産省'19]	Value Creation Process	サイバー空間とフィジカル空間の両空間を跨いで、様々なモノやデータが動的につながって構成される付加価値の創造活動。
4	信頼	Trust	利用者又は他の利害関係者がもつ、製品、システム、サービスが意図したとおりに価値を提供するという、確かな期待。信頼性にもとづく期待。
5	信頼性	Trustworthiness	セキュリティ、プライバシー、セーフティ、リライアビリティ、レジリエンスなどによって、システムがその関係者の期待に応える能力 参考： ISO/IEC JTC1/WG13 "For supply/value chain security and risk management, the term 'Trustworthiness' corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way."
6	(信頼の)証明	Prove, Proof	Value Creation Process のソシキ、ヒト、モノ、データ、システム、プロセスの6つの観点について必要な規程が満たされていることを、第三者により確認されていること。
7	OEM [JETRO '17]	Original Equipment Manufacturer	委託者のブランドで製品を生産すること、または生産するメーカーのこと
8	サプライチェーン [ISO28001 : 2007]	Supply Chain	原材料の調達から始まり、製品の製造、加工、配送、および消費者への製品提供やサービス提供にまで至る、発注指示される一連のリソースとプロセスである。 注)サプライチェーンの担い手として、ベンダ、製造施設、ロジスティクスプロバイダ、内部流通センタ、流通業者、卸売業者、および商品とその関連サービスの製造または提供過程、処理、取り扱い、配送または提供に関与する者が含まれる場合がある。
9	プロシージャ [経産省'19] [TaaS WP '21]	Procedure	[経産省'19] 定義された目的を達成するための一連の活動の手続き [TaaS WP '21] 産業活動・サービス・手続き等における目的を実現するための、相互に関連するまたは相互に作用する一連の活動、手順を表す。
10	デジタル化 (デジタル化とデジタルトランス)	DX : Digital Transformation	企業が外部エコシステム(顧客、市場)の破壊的な変化に対応しつつ、内部エコシステム(組織、文化、従業員)の変革を牽引しながら、第3のプラットフォーム

項番	用語	英語表記	説明
	フォーメーションは一般には意味が異なるが、本書ではデジタルトランスフォーメーションをデジタル化と表現する)		(クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術)を利用して、新しい製品やサービス、新しいビジネス・モデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること
11	MaaS	Mobility as a Service	MaaS(マース：Mobility as a Service)とは、地域住民や旅行者一人一人のトリップ単位での移動ニーズに対応して、複数の公共交通やそれ以外の移動サービスを最適に組み合わせて検索・予約・決済等を一括で行うサービスであり、観光や医療等の目的地における交通以外のサービス等との連携により、移動の利便性向上や地域の課題解決にも資する重要な手段をさす。
12	トラストストア [IIC '21]	Trust Store	信頼できるサプライチェーンを構成する組織ごとに、デジタルエビデンス(本誌では実施確認結果)が、それぞれの組織のシステムによって、トラストストアと呼ばれる共有情報システムに公開される。トラストストアは信頼性を示すデータを保存し、参加者が利用できるようにする。
13	TaaS [TaaS WP '21]	Trust as a Service	フィジカル空間の手続きをデジタル化するために、サイバー空間に必要なトラストを実現するための機能。相手先信頼レベル確認、モート型データ完全性、リモート型プロシージャ・システム正当性、任意の第三者による検証、利用者の負担軽減を実現する仕組み(UX)に対応する機能を有する。サービス型として提供される。
14	ベース・レジストリ [包括的データ戦略'21]	Base Registry	公的機関等で登録・公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データ 51 種であり、正確性や最新性が確保された社会の基盤となるデータベース
15	トラストサービス	Trust Service	インターネットにおける人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み 参考: 総務省「プラットフォームサービスに関する研究会の最終報告書」, https://secure-web.cisco.com/13ugQHllJSNajvVsa7MyaQrpnURxK3PIcIQ7oDR0lfFZuDPjAQyTmWZiu6HorOV7rNyx3IWWPZ_zjnmwFbVf2o-suJRpfTtrOjqkOdxLlvYjXmSKG2nVPWniyyjNt9JuVzjzZS5f3NWB0nPTvJXgjeBGsKN2HGKA-bh8a30FDZlpnDTRnzroArCDUL3SxtG7pnzgYRcn-l7Bg53_ZmL4RsITGRvI0cY8WnaEE6gglyTMnVQAiSPnKWvmzqqnvUc3uzli3ABsTf1jULmwDgCniO6qjpZaQoAf5asRLvGCJFXJ4W2P0G2QZx0L-Vb7we_fmBms5z5EvPH_m7pYoebd9w/https%3A%2F%2Fwww.soumu.go.jp%2Fmain_content%2F000668595.pdf

II. スコープ：安心・安全に向けたサプライチェーンのトラスト

近年、インターネットが経済や生活に浸透する中で、クラウドサービス、人工知能(AI)、IoT 等によるデータ主導のデジタル社会つまり Society 5.0 が到来しつつある。Society 5.0 はサイバーとフィジカルが高度に融合し、人、組織、モノ、データ、プロシージャ、システムが複雑に関与しあって価値(製品、サービス、データ)を創出する世界(社会)である[経産省'19]。このようにデジタル化が進み、あらゆるモノ、コトがデータでつながる世界においてサプライチェーンのトラストを確保し、安心・安全な Society 5.0 を実現することが、本ホワイトペーパーのスコープである。

- サプライチェーンにおける価値(製品、サービス、データ等)の創出過程が期待どおりであること
- サプライチェーンで創出された価値(製品、サービス、データ等)が期待どおりであること
- サプライチェーンを通じて価値(製品、サービス、データ等)が、アフターサービスも含めて期待どおり提供され続けること

III. 環境状況/状況の変化

前章で述べたスコープの認識のもと、サプライチェーンに関する環境状況/状況の変化を(動向1)から(動向4)にまとめる。

(動向1) サプライチェーンやアフターサービスのデジタル化

サプライチェーンを構成する組織では、企業間取引、製品やサービスの製造や提供過程、保守メンテナンス、リモート監視を含めたアフターサービスにおいてデジタル化が進んでいる。また機器、センサなどから取得されるデータを活用した設備の運用・保守メンテナンスなど新しいサービス提供も加速している。

(事例1-1) 製造過程のデジタル化

工作機械メーカーの製造工程のデジタル化が進み、顧客の製品の加工や試作のデータを共有し、テスト加工や試作を3次元の仮想空間で行われるようになってきた。この仮想空間での加工や試作を通じ、顧客とのつながりを持つことで、ビジネス機会を増やす取り組みが行われている⁴。

(事例1-2) 企業間取引のデジタル化

2019年の日本国内の企業間(BtoB)電子商取引の市場規模は353兆円であり、前年比2.5%に拡大した。また、商取引金額(商取引市場規模)に占める電子商取引市場規模の割合も増加傾向にあり、商取引の電子化が引き続き進展している⁵。

(事例1-3) アフターサービスのデジタル化

機器等から集められた産業データを元にしたビジネスが拡大している。i-Construction と呼ばれ、建設現場のICT 建設機器からの作業実績情報、ドローンからの作業現場地形の3次元計測情報など様々なデータを蓄積、解析することで、施工状況のリアルタイム管理や進捗状況の共有を可能にするシステムの導入が進んでいる⁶。

また、石油・化学や電力・ガス等の産業・エネルギー、エレベータ・ビルなどの関連インフラ事業者は、設備の経年劣化や人材の高齢化により、長期的な人材不足、技術・技能伝承力の低下という問題に直面している。これらの問題に加え、近年の日本では災

⁴ DMG 森精機、工程8割デジタル化 仮想空間で部品試作: 日本経済新聞 (nikkei.com)

<https://www.nikkei.com/article/DGXZQOFD0834A0Y1A800C2000000/>

⁵ 経済産業省 電子商取引に関する市場調査の結果を取りまとめました

<https://www.meti.go.jp/press/2020/07/20200722003/20200722003.html>

⁶ データ利活用の事例集 Case03 Platformer①

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/data_jireisyu.pdf

害が激甚化し、災害に対応した高い安全性を有する設備への要求にも直面している。デジタル技術を活用して、インフラ関連設備の機器のセンサから出るデータを使い、設備の修繕や交換が必要な箇所の診断や監視を自動化し、省人化を図りながら、高い安全性を確保するサービスの導入が進んでいる⁷。

(動向2) ニーズの多様化や外部状況変化に対応した製品やサービスの価値の継続的な供給

消費者の求めるニーズの多様化や、外部状況などの変化に柔軟に、かつ迅速に対応し、製品やサービスの価値を継続的に供給するためのサプライチェーンを構成する組織によるさまざまな取り組みが行われている。

(事例2-1) 消費者ニーズの多様化に対応した製品やサービスの継続的な供給

ビジネス向け PC は CPU、メモリ、HDD などのカスタマイズのニーズが高い製品である。このニーズに対応するため、ビジネス向け PC を供給する事業者は、購入 Web サイトで細かくカスタマイズ要求を受け付け、工場ですべての要求にあったビジネス向け PC を組み立てる、というサプライチェーンを組んでいる⁸。

(事例2-2) 外部状況の変化に対応した製品やサービスの継続的な供給

東日本大震災にみまわれたときに東北地方にあった部品メーカーが被災し、自動車メーカーは必要な部品の確保ができなくなった。このときに判明したことが、サプライチェーンの構造が、従来 OEM を頂点にした系列のサプライヤからなる構造ではなく、ひとつのサプライヤが複数の系列に属する構造をとっていたことであった⁹。自動車メーカーはトータルサプライチェーンの可視化、地域的リスク回避、パートナー工場の設備状況の把握などに着手し、危機時においてもサプライチェーンを寸断させないためのリスク分散を進めた。

(事例2-3) ソフトウェア部品としてのオープンソースソフトウェアの活用

ソフトウェア開発の現場では、機能性や利便性の点からオープンソースソフトウェアの活用が進んでいる。従来はソフトウェア製品として提供されてきたものが、近年はニーズに柔軟に、かつ迅速に対応するためにオープンソースソフトウェアに代替することが増えている。

⁷ スマート保安指針のための基本方針 経済産業省 令和2年

https://www.meti.go.jp/shingikai/safety_security/smart_hoan/pdf/kihon_hoshin.pdf

⁸ ものづくり.com 「BTO」とは https://www.monodukuri.com/gihou/article_list/125/BTO

⁹ 経済産業省 METI 「ものづくり白書2019 第1部 ものづくり基盤技術の現状と課題 第1章 平成の製造業とものづくり白書の変遷」

https://www.meti.go.jp/report/whitepaper/mono/2019/honbun_pdf/index.html

(動向3) サプライチェーンの構造の変化とサプライヤの参入業種の多様化、製品やサービスの供給ルートの複雑化

サプライチェーンでは、サプライヤの参入業種が多様化するとともに、製品やサービスの供給ルートの複雑化も進んでいる。

(事例3-1) ピラミッド構造からダイヤモンド構造へ

自動車メーカーでは、部品の供給の効率化、低コスト化を推進した結果、中核部品である半導体チップの供給が、系列外の特定のサプライヤに集中している場合がある。この場合のサプライチェーン構造は、ひとつのサプライヤが複数の系列に属するような、水平分業型のダイヤモンド構造となっている⁹。

(事例3-2) 異業種・サービスを含めたダイヤモンド構造

自動車保険において車載機器からデータを取得し安全運転者の保険金を安くするようなテレマティクス保険サービスが提供されており、これにより車載機器を開発するメーカーや、データ収集を請け負うサービスといった新たなサプライヤが誕生した。これらのサービスでは、自動車メーカーや保険会社といった従来のサプライヤに限らず、新たなサプライヤが参入し、製品やサービスの供給ルートも複雑化してきている¹⁰。

(動向4) サプライチェーン全体で遵守が求められるルール形成の加速

OEMのそれぞれでルールを遵守することは当然であるが、近年は、サプライチェーンを構成するサプライヤの全てでルールに従っていることの説明を求められている。このようなルールがグローバルに次々と形成されている。

(事例4-1) GDPR

2018年から欧州連合において、個人が自分の個人データを管理する権利を取り戻し、欧州連合内の規則を統合することを目的に作られたGDPR(General Data Protection Regulation, 一般データ保護規則)が適用された。GDPRでは、委託された業者が個人データを処理する場合にも、データ処理業務にてGDPRを遵守していることの説明責任をデータ管理者に課している。GDPRに違反した場合、企業には巨額な制裁金が課せられる¹¹。企業がGDPRを遵守していることの説明責任を果たすとき、サプライヤも同様に説明責任を果たす必要があり、そうした全体での説明責任を果たせないと制

¹⁰ 国土交通省 日本版 MaaS の推進 MaaS モデルの形成

<https://www.mlit.go.jp/sogoseisaku/japanmaas/promotion/model/index.html>

¹¹ 日本貿易振興機構 ビジネス短信 GDPR 適用開始から2年、域外適用の範囲を明示

<https://www.jetro.go.jp/biznews/2020/06/c81164d22cfa1274.html>

裁金を課せられるリスクが増す。

(事例4-2)WP29

自動運転車のセキュリティ要件が、WP29(自動車基準調和世界フォーラム)にて策定され、自動車メーカーが自動運転車を設計、開発、製造するときに盛り込むべきセキュリティ要件が合意された¹²。自動車メーカーは、このセキュリティ要件を製品が満たしていることを説明する必要がある。製品がセキュリティ要件を満たしていることを説明する際、メーカーのサプライヤ側でも同様に、セキュリティ要件を満たしていることを説明しなくてはならない。WP29 のセキュリティ要件を満たしていることを説明できないと、量産品の検査の工数低減に必要な型式指定を取り消される可能性や、車両の量産ができなくなる可能性がある。

(事例4-3)SDGs

2015年の国連で2030年までの国際開発目標であるSDGs(Sustainable Development Goals, 持続可能な開発目標)が採択された。17の目標と169のターゲット達成が示されており、企業はこの中から目標を設定、公開し、達成に向けて継続的な対応を行う¹³。企業がSDGsへの取り組みを説明することは、社会的な企業価値を示すものとして重要になってきている。SDGsへの取り組みを説明するには、OEMは自社でのSDGsへの取り組みの説明だけでなく、サプライヤのSDGsへの取り組みも含めて、サプライチェーン全体で説明しなくてはならない。

(事例4-4)ESG

近年では、環境(Environment)、社会(Social)、ガバナンス(Governance)三つの観点から企業を分析して投資する「ESG投資¹⁴」が注目されている。企業が投資を受ける際、将来の企業価値を示すものとしてESGへの取り組みを説明することが重要になってきている。ESGへの例として、環境負荷の少ない部材やエネルギーを使うことや、廃棄プロセスでの環境負荷を少なくするなど、OEMだけでなくサプライヤも含めたサプライチェーン全体で、ESGへの取り組みを説明しなくてはならない。

¹² 国土交通省 報道・広報 「自動運転技術に関する国際基準等を導入します ～道路運送車両の保安基準等及び保安基準の細目を定める告示等の一部改正について～」

https://www.mlit.go.jp/report/press/jidosha10_hh_000242.html

¹³ 経済産業省 SDGs https://www.meti.go.jp/policy/trade_policy/sdgs/

¹⁴ 経済産業省 ESG 投資

https://www.meti.go.jp/policy/energy_environment/global_warming/esg_investment.html

IV. 解決すべき課題

サプライチェーンの動向や変化として前章は以下の4つを述べた。

- (動向1) サプライチェーンやアフターサービスのデジタル化
- (動向2) ニーズの多様化や外部状況変化へ対応した製品やサービスの価値の継続的な供給
- (動向3) サプライチェーンの構造の変化とサプライヤの参入業種の多様化、製品やサービスの供給ルートの複雑化
- (動向4) サプライチェーン全体で遵守が求められるルール形成の加速

こうした中でサプライチェーンのトラストを確保するため、本章は解決すべき(課題1)から(課題4)を述べる。

(課題1) デジタル化にともなうデータのセキュリティ脅威への対応

サプライチェーンを構成する組織では、工場やプラントが自律的に大量のデータを扱うようになり、モノづくりの信頼性、データを活用したサービスの信頼性が、「データの信頼性」に強く依存するようになってくる。デジタル化したデータは常にセキュリティの脅威にさらされ、データの生成された日時や場所や発信元を確認したり、やり取りの途中で改ざんやすり替えがされていないことを確認したりすることは困難である。さらにサービスがデジタル化するとその手続きで使われるデータも脅威にさらされ、データの生成元や生成日時、改ざんやすり替えがされていないことの確認も困難となる。製品の製造過程やサービスの提供過程で生成される設計データやプロセスデータ、企業間取引の取引データ、インフラ設備データは、現実世界の製品やサービス、企業間の取引、設備の稼働状況と密接に関係する。そのためデータの信頼性の確保が、現実世界の製品やサービス、企業間取引、設備の稼働の信頼性に影響する。しかしながら、「信頼できるデータ」について、日本国内でコンセンサスが得られた基準やガイドラインが存在しないため、国際動向や技術動向と比較して不適切な基準で運用されているサービスが存在する恐れがある。

(課題2) ニーズの多様化や外部状況の変化に対応してサプライヤを容易に組み替えることができない

サプライチェーンを構成する組織が新たなニーズや外部状況の変化に対応するには、サプライチェーンに新たなサプライヤを取り込むような、サプライチェーンの組み替えが必要になる。サプライヤの提供する製品やサービスが新たなニーズや外部状況の変化に見合ったと確認するには、そのサプライヤの実績や能力、適切な管理がなされているか等を確認する必要があり、これには時間とコストがかかる。より良い機能性や利便性を備えた製品やサービスを新たなサプライヤが提供できると主張しても、その主張が新たなニーズや外部

状況の変化に見合ったものであることを確認するには、時間とコストがかかる。

(課題3) サプライチェーンの複雑化で問題発生時の原因特定と影響範囲の把握が困難

サプライチェーンを構成する組織は、サプライヤの業種の多様化や、供給ルートの複雑化が進むと、最終製品やサービスに問題が発覚した時に、問題の原因がサプライチェーンのどこにあるかを特定することが困難になる。さらに、その原因が他の製品やサービスにまで影響するかどうか(影響範囲)を適切に判断することも困難である。問題の原因特定や影響範囲の特定に時間がかかると、製品提供やサービス復旧が遅れ、ビジネス機会の損失や企業イメージの棄損につながる。

(課題4) サプライチェーン全体でのルール遵守や新たな価値観への対応状況の説明

サプライチェーンを構成する組織は、サプライチェーン全体に課せられるルールが次々と形成されるなか、これらのルールに従わなくてはならない。これらルールに従うためにサプライチェーンに適用する規程を OEM 自ら策定し、サプライヤはこれに従って企業活動に取り組む必要がある。サプライチェーン全体でルールを遵守していることを説明できないことは、ビジネスの機会損失や制裁金を課されるといったリスクにつながる。

さらに、社会の持続的成長に向けて、SDGs や ESG のような新たな社会価値・環境価値向上につながる取り組みが企業に求められている。企業イメージや企業価値を高めるためには前述のルールへの対応と同様に、サプライチェーンに適用する規程を自ら策定し、社会価値・環境価値向上に取り組んでいることを適切に説明できなければならない。

これらの課題を解決するための方策を次章に述べる。

V. 解決に向けた方策

1. サプライチェーンのトラストのめざす姿

前章に記載した課題を踏まえて、サプライチェーンのトラストのめざす姿を以下に述べる。

(めざす姿1) サプライチェーン全体で生成、やり取りされる、データの信頼性を容易に確認できる

サプライチェーンを構成する組織は、データの生成元を確認でき、その後も改ざんなどが無いことを確認できる。さらにサービスに使われるデータも、同様の確認を容易にできる。これらにより、データに基づいて提供される現実世界の製品やサービスの信頼性も容易に確認できる。

(めざす姿2) ニーズや外部環境の変化に応じて適切なサプライヤを選択できる

サプライチェーンを構成する組織は、新たなサプライヤの実績や能力、適切に生産や販売を管理しているか等の確認を時間とコストをかけずに行うことができる。これにより適切にサプライヤを選定でき、サプライチェーンに新たなサプライヤを取り込むような、サプライヤの組み替えを容易に行うことができる。その結果、多様なニーズや外部環境の変化に対応できる。

(めざす姿3) サプライチェーンの構造を容易に把握できる

サプライチェーンを構成する組織は、サプライヤの業種が多様化し供給ルートが複雑化しても、最終製品やサービスに問題が発覚した時に、問題の原因がサプライチェーンのどこにあるかを容易に特定できる。さらに、その原因が他の製品やサービスにまで影響するかどうか(影響範囲)を適切かつ容易に判断できる。問題の原因特定や影響範囲を容易に特定できることで、早期に製品提供の再開やサービスを復旧でき、ビジネス機会損失や企業イメージの低下を回避できる。

(めざす姿4) サプライチェーン全体でのルール遵守を説明できる

サプライチェーンを構成する組織は、次々と形成されるサプライチェーン全体に課せられるルールに対し、サプライチェーン全体で遵守していることを説明できる。サプライチェーンに適用する規程を自ら策定し、この規程に従って企業活動に取り組むことで、ビジネスの機会損失や制裁金を課されることを回避できる。

さらに、社会の持続的成長に向けて、SDGs や ESG のような新たな社会価値・環境価値向上につながる取り組みを説明できる。企業イメージや企業価値を高めるために、サプライチェーンに適用するより高い目標を規程として策定し、その規程を実施し、その高い目標を達成したことを説明できることで、企業価値を高めることができる。

2. 要件

前節でサプライチェーンのトラストのめざす姿を述べた。本節ではめざす姿1～4を達成するための要件を述べる。

(要件1) サプライチェーン上でやり取りされるデータの信頼性を容易に確認できる

- (要件1-1) サプライチェーンで生成・やり取りされるデータの、生成日時や場所や発信元と、改ざんやすり替えがないことを容易に確認できる。
- (要件1-2) データの生成元の信頼性を確認できる。例えば、データの生成元である組織や人や機器が、実際に存在することや、詐称していないことを容易に確認できる。

(要件2) 製品の製造過程やサービスの提供過程に課せられる規程と、規程に従い実施されたことを容易に確認できる

- (要件2-1) 製品の製造過程やサービスの提供過程に課せられる規程を、容易に確認できる。
- (要件2-2) 規程に従い実施されたことを容易に確認できる。

(要件3) サプライチェーンを構成する組織、製品やサービスのつながりを容易に確認できる。

- (要件3-1) サプライチェーンを構成する組織のつながりを容易に確認できる。
- (要件3-2) 製品やサービスの生成、供給ルートを確認できる

3. 実現方法

3-1. サプライチェーンのトラストの分類

サプライチェーンのトラストが形成される範囲は、「期待に応える能力をどの範囲で検証できるか」に依存する。トラストが形成される範囲は、検証をおこなう主体(組織・人)の範囲に応じて、以下の(1)(2)に分類される。

(1)プライベートトラスト

特定の限られた範囲における主体間で、期待に応える能力を検証できることにより形成されるトラスト

(例)組織内、組織間(発注者 - 受注者など)、業界団体といった、特に参加・脱退のプロセスがある関係性。

(2)パブリックトラスト

範囲を限定せずに、主体の期待に応える能力を検証できることにより形成されるトラスト

(例) 国、国家間など、明示的な参加・脱退のプロセスがなく公共性があるもの。

3-2. 実現方法の全体像

サプライチェーンのトラストを実現するための全体像を図 V-1 に示す。トラストを実現するために「トラストストア」「デジタルエビデンス」「TaaS (Trust as a Service)」「ベース・レジストリ」を用いる。

サプライチェーンを構成する人、組織、モノ、データ、プロシージャ、システムの信頼性の根拠となる情報をデジタルエビデンスとして記録し、信頼性を示す情報と、それらのつながりを示す情報をトラストストアに格納する。サプライチェーンおよびトラストストアにおけるデータを、TaaSを通じて送受信することにより、データの真正性と完全性、さらにはデータの生成元である人、組織、モノの実在性を担保する。さらにベース・レジストリを活用して、サプライチェーンを構成する人、組織、モノ、データ、プロシージャ、システムを指し示す再利用性の高いデータに対して、正確性や最新性を担保する。

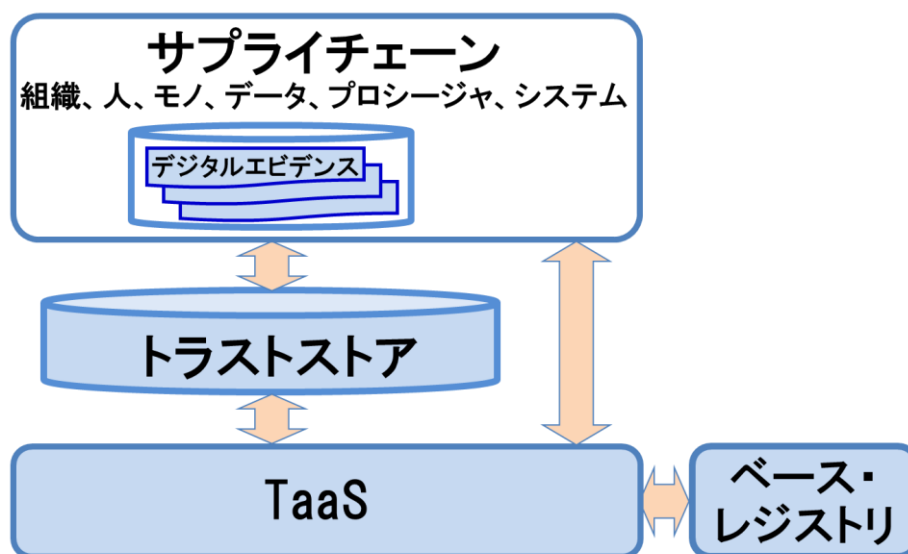


図 V-1 サプライチェーンのトラストを実現するための全体像

表 V-1 サプライチェーンのトラストを実現するための構成要素

#	構成要素	説明
1	トラストストア	サプライチェーンを構成する人、組織、モノ、データ、プロセス、システムの信頼性を示す情報と、それらのつながりを示す情報を格納したもの
2	デジタルエビデンス	予め合意された規程に基づいて実施されたことを確認した結果の根拠になる情報
3	TaaS	データの真正性および完全性を検証できるようにする。データが示す人、組織、モノの実在性を検証できるようにする
4	ベース・レジストリ	再利用性が高いデータの正確性や最新性を担保する

次にトラストストア、デジタルエビデンス、TaaS、ベース・レジストリのそれぞれの概要と実現方法を説明する。

3-3. トラストストア、デジタルエビデンス

(1)概要

トラストストアとデジタルエビデンスは、Industrial Internet Consortium 発行の「The Industrial Internet of Things Trustworthiness Framework Foundations, Version V1.00” (2021.7.15)」[IIC ‘21]の中で、サプライチェーンでのトラストを構築するために導入された概念である。トラストストアとデジタルエビデンスの概要を、図 V-2 に示す。

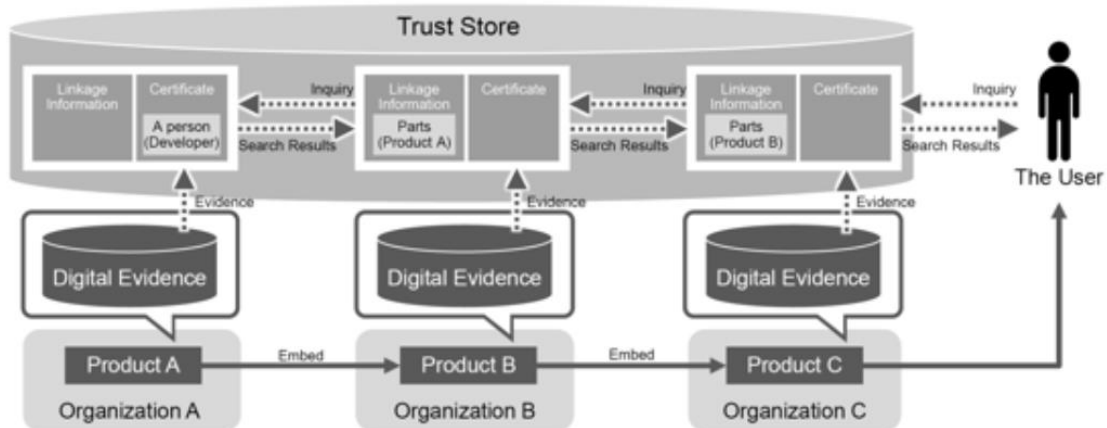


図 V-2 サプライチェーンでのトラストストアとデジタルエビデンスの概要([IIC '21]Figure4-8)

サプライチェーンは、製品やサービスの製造や提供過程、企業間取引、保守メンテナンスなどのライフサイクルにわたって構築される。トラストストアは、サプライチェーンを構成する組織(図中の Organization A, B, C)が、組織のアウトプットとなる製品やサービス(図中の Product A, B, C)を期待どおりに提供していることを示す証明書(図中の Certificate)を格納するものである。さらに、組織間の取引のつながり、製品の構成部品や材料のつながり、サービスの需給のつながりを示した紐づけ情報(図中の Linkage Information)を証明書に付加して、証明書に記載された組織や製品やサービスのつながりを辿ることができる。格納された証明書は、製品やサービスの製造過程や提供過程が期待どおりに実施したことの根拠となるデジタルエビデンス(図中の Digital Evidence)によって裏付けることで、製品やサービスを期待どおりに提供していることを示している。

(2) 実現方法

サプライチェーンのトラストの実現にあたり、トラストストアの利用方法を、図 V-3 に示す。サプライチェーンのトラストを実現するための要件 2 および要件 3 を、トラストストアにおける証明書と紐づけ情報により実現する。

トラストストアはサプライチェーンにおいてサプライチェーンを構成する人、組織、モノ、データ、プロシージャ、システムの信頼性を示す情報と、それらのつながりを示す情報を格納したものである。

組織の製品やサービスの製造過程や提供過程を予め規程として定め、その規程を基に実施したログを確認し、それをデジタルエビデンスとして証明書と対応づける。トラストストアに格納された証明書は、製品の製造過程やサービスの提供過程に課せられる規程と、規程に従い実施されたことを示すものである。サプライチェーンを構成する

組織や消費者は、証明書に対応づけられたデジタルエビデンスにより、規程に従い実施されたことの根拠を確認できる。

また、証明書とその証明書に付加された紐づけ情報により、サプライチェーンを構成する組織、製品やサービスのつながりを容易に確認できる。

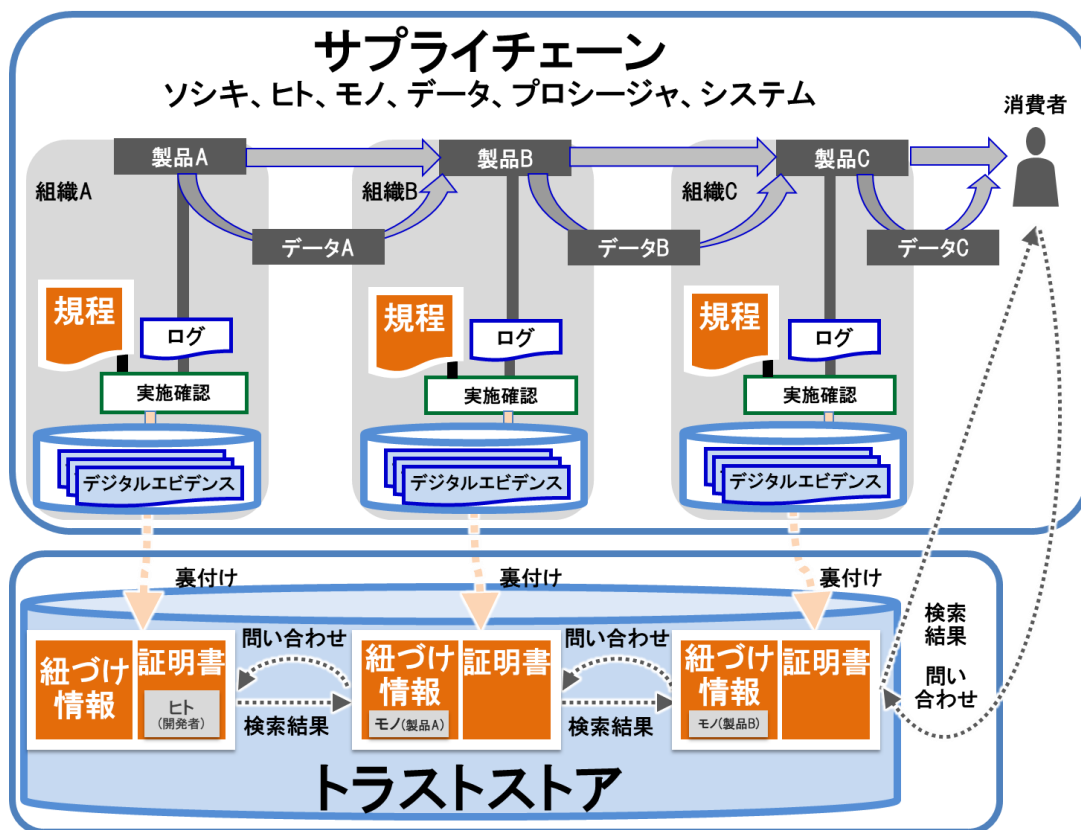


図 V-3 トラストストアの利用方法 ([IIC '21]Figure4-8 に加筆)

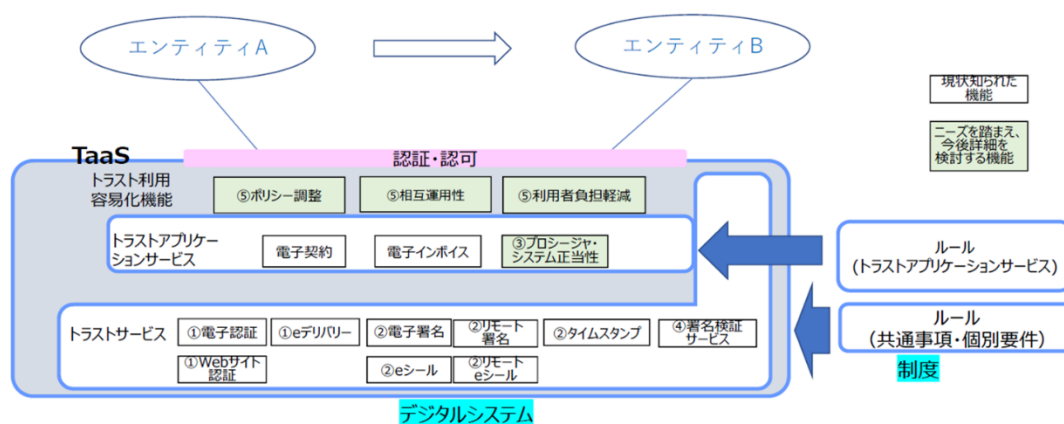
なお、図 V-2、図 V-3 では、1つのトラストストアで記載しているが、その実装形態に限らず、トラストストアは、企業単位、或いは業界単位など複数の実体により構成される場合も考えられる。その場合でも、企業や業界を跨って上記と同様のことが実現できなければならない。

3-4. TaaS

(1)概要

TaaSとは、デジタルトラスト協議会ルール形成委員会発行の「ホワイトペーパー第1版(2021.12.7)」[TaaS WP '21]の中で以下の図 V-4 に示すよう定義している。

TaaSとはサイバー空間でのデータのトラストを実現する電子認証、電子署名、リモート署名、eシール、タイムスタンプ等のトラストサービスの上に構築される。トラストサービスは、書面・押印のデジタル化に伴う制度的な有効性を支える。またTaaSは利用容易化機能を有し、TaaSを利用する人、組織、モノ、システムに対して、リモート型サービス等の利用容易性を実現することで、堅確性を実現する。利用容易化機能は、トラストサービスと連携することで、制度的な有効性に支えられた堅確性を実現する。さらにトラストアプリケーションサービスを有し、電子契約や電子調達等、特定の業務に関連したサービスを提供する。このトラストアプリケーションサービスは、トラストサービス、もしくは利用容易化機能と連携することで、トラストアプリケーションで対象とする特定業務に関して、制度的な有効性に支えられた正確性および確実性を実現する。このTaaSを用いて、データがすり替えられていないことである真正性、データが改ざんされていないことである完全性、相手が実在していることである実在性が担保されていることを確認できる。



トラストアプリケーションサービス：トラストサービスの応用サービス
 トラストサービス：電子認証、電子署名、リモート署名、eシール、タイムスタンプ、eデリバリー、Webサイト認証、および署名検証サービス、等を指す
 トラスト利用容易化機能：トラストアプリケーションサービス、システム・サービス、および実空間から自らの目的に合わせて、トラストサービスを容易に利用するための補助機能

図 V-4 TaaS の仕組み([TaaS WP '21] 図 1 5 より引用)

(2)実現方法

サプライチェーンのトラストにおける前節で述べた要件1を、TaaSを用いて実現する。サプライチェーンを構成する組織や消費者は、トラストストアに格納された証明書や紐づけ情報の真正性および完全性を、TaaSを用いて検証する。また、データの生成元である人、組織、モノの実在性を、TaaSを用いて検証する。このようにTaaSを用

い、サプライチェーン上でやり取りされるデータやデータの生成元の信頼性を容易に確認できる。

3-5. ベース・レジストリ

(1)概要

ベース・レジストリとは、2021年6月に政府から出された「包括的データ戦略」[包括的データ戦略'21]の中で、「公的機関等で登録・公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データであり、正確性や最新性が確保された社会の基盤となるデータベース」と定義されている。

(2)利用方法

サプライチェーンのトラスト実現に向けたベース・レジストリの利用方法を図 V-5 に述べる。ベース・レジストリはTaaSを介して、サプライチェーンを構成する組織や消費者により利用されるものである。例えば法人のベース・レジストリを確認することで、取引相手の実在性や、プライバシーマークなどの属性情報や、購買手続きにおいて用いるデータなど、再利用性の高いデータを中心に、正確で最新の情報を確認することが可能になる。

・法人活動の確認に関する確認

取引相手の実在性確認に加えて、公開された属性データ（プライバシーマーク、ISO 9000,14000等）、購買手続きにおいて用いるデータ等を参照するトラスト基盤を、法人のベース・レジストリとの連携により実現。

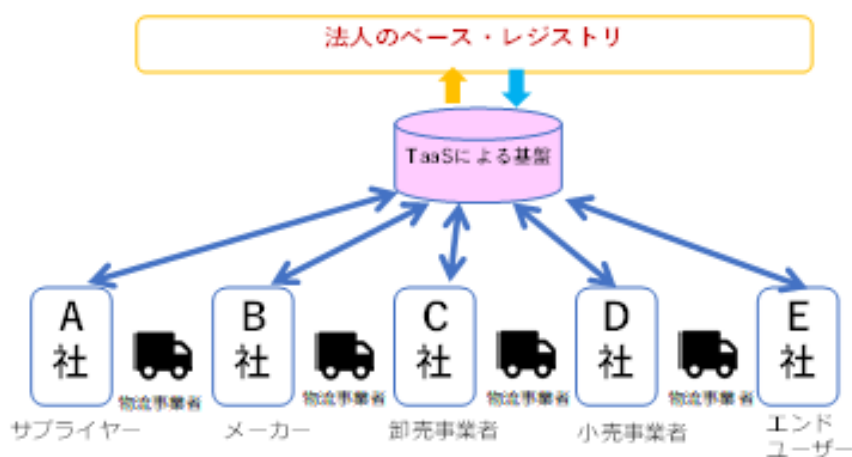


図 V-5 サプライチェーンのトラスト実現に向けたベース・レジストリの利用方法 ([TaaS WP '21]図 25 より引用)

3-6. サプライチェーンのトラスト要件との関係

前節では、サプライチェーンのトラストにおける要件として以下の3つを述べた。

- (要件1) サプライチェーン上でやり取りされるデータやデータの生成元の信頼性を容易に確認できる。
- (要件2) 製品の製造過程やサービスの提供過程に課せられる規程と、規程に従い実施されたことを容易に確認できる。
- (要件3) サプライチェーンを構成する組織、製品やサービスのつながりを容易に確認できる

サプライチェーンのトラストを実現するための要件と、トラストストア、デジタルエビデンス、TaaS、ベース・レジストリとの関係は以下のとおりである。

- (要件1)→ TaaS とベース・レジストリによってデータやデータの生成元の信頼性を容易に確認できる。
- (要件2)→ トラストストアとデジタルエビデンスによって規程と、規程に従い実施されたことを容易に確認できる。
- (要件3)→ トラストストア、デジタルエビデンスによってサプライチェーンを構成する組織、製品やサービスのつながりを容易に確認できる。

4. ユースケース

以下にユースケースを述べる。

4-1. 機器から出るデータの信頼性を確保する仕組み

トラストの概要

近年、石油・電力・ガス等の社会インフラや、ビル、工場においては、IoT や AI 等の新技術を活用し、遠隔地から常に状態を把握・監視し機器や設備の状態を診断し、安全性、効率性の向上を図るケースが増えてきている。例えば、製造業者は、自社が製造した製品を事業者に納入し、製品の遠隔監視や、製品から出るデータを解析し、異常を予兆段階で検知する予兆検知システムがある。この予兆検知システムにより、故障や事故を未然に防止すると共に、設備の余寿命をより正確に予測し、適切なタイミングで修繕・交換を実施する保守・メンテナンスサービスを提供する。このようなケースでは、データの取得先、データの取得タイミング、または製品から生成されるデータが誤っていると、診断結果も誤ったものとなる。また、誤った診断結果に基づいて不適切な対応を行ったことで、業務停止を引き起こすと、保守メンテナンスサービスの信頼も失ってしまう。そのため、製造業者は、製品から出るデータの信頼性の確保が重要となる。

Before(課題)

製造業者は、事業者が使用している製品から取得したデータが、信頼できるデータであるかどうかを確認、検証ができない。例えば、上記で示した保守・メンテナンスサービスの提供において、どういう要素や要件を満たせば、信頼できるデータであると言えるのか、どのレベルの信頼性が求められるのか判断するための基準やガイドラインが、現在存在しない。また、製造業者は製品から取得したデータに基づいて提供するサービスが信頼できるデータを元に提供していると第三者に示すこと、または検証ができない。そのため、国際動向や技術動向と比較して不適切な基準で運用されているサービスが存在する恐れがある。

After(めざす姿)

製造業者や事業者は、事業者が使用している製品から取得したデータに基づいて実施する作業やサービスが、信頼できるデータに基づいて行われていることを、政府等が発行するガイドラインを元に第三者に示す、または検証することができる。ガイドラインには、産業分野、事業形態に応じて必要とされる信頼性のレベルが提示され、そのレベルごとに必要な要件や基準が規定されており、企業は信頼性が確保されているサービスを提供できる。

実現方法

保守メンテナンスサービスのケースを用いて、「信頼できるデータ」の実現例を説明する。「信頼できるデータ」の実現には、図 V-1 に示したサプライチェーンのトラストの実現方法のうち、図 V-6 に示すように TaaS を用いて実現する。

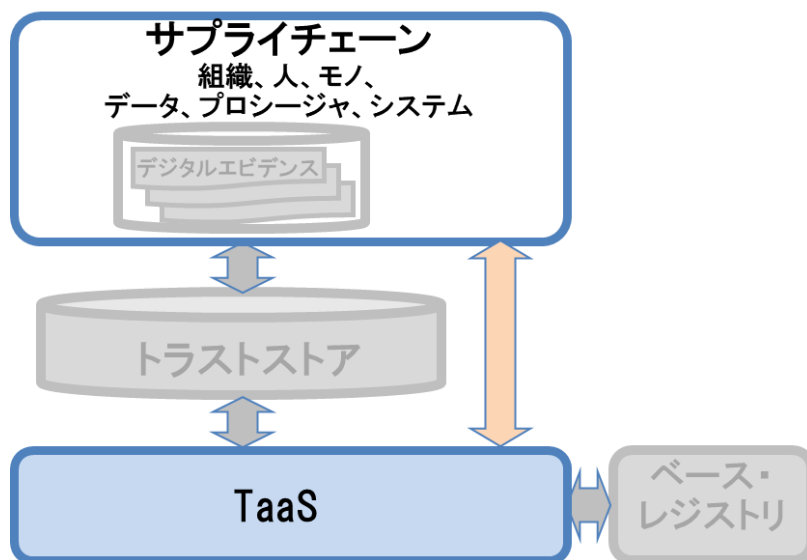


図 V-6 本ユースケースでのサプライチェーンのトラストの実現方法

機器から出るデータの信頼性に必要な要素が定義されており、その要素を満たしたサービスを事業者が提供するユースケースを下記に提示する。

製造業者 A は、自社が製造した製品 A' を事業者 B に納入し、製品 A' を遠隔監視、製品 A' から出るデータを元に保守メンテナンスサービスを提供。事業者 B は、製品 A' 機器から出るデータの信頼性に必要な要素を定義し、それを実現する。信頼性に必要な要素は以下の(i)(ii)である。

(i) 機器から出るデータの信頼性に必要な要素の定義

2021年6月に政府から出された「包括的データ戦略」[包括的データ戦略'21]においては、フィジカル空間をサイバー世界のデータに置き換えるための「データのトラストの要素」について述べられている。その「データのトラストの要素」では、誰が(主体・意思)、何を(事実・情報)、いつ(時刻)というフィジカル空間の構成要素を正しくサイバー空間でも「トラストの要素」として再現することが必要と言及している。

このため、フィジカル空間にある“機器”から出るデータをサイバー世界のデータに置き換えトラストを確保するためには、(ア)誰が(イ)何を(ウ)いつの構成要素のトラストが必要と考えられる。

(ア)機器の利用者(組織)が正しいこと

- ・ 機器を利用している「組織」が正しいこと(機器を利用する主体の信頼性の確保)
例)電子署名の活用

(イ)機器が正しいこと

- ・ 「機器」が存在するという事実の確認、「機器」の信頼性の確保
- ・ 機器を製造した製造ベンダが(機器の仕様(セキュリティ含む)と製造プロセス、バージョン/アップデートなどが正当であることを)保証
- ・ 信頼できる製品とは、
 - (あ)信頼できる製造業者が作った製品
 - (い)信頼できる製造業者しか作成できない証明書に対応する秘密鍵が入っている製品
 - 例) 信頼できる製造業者が出荷前に組み込んだアクティベート用の鍵を使って、データ用の鍵を設定
 - 例) eシールの活用(eシール用電子証明書の拡張領域に記載する)
※機器のIDの発効主体については、ユースケース、求められるトラストのレベルに応じて異なる(後述)

(ウ)「存在・時刻」 機器から生成されたデータの時刻が正しいこと

- ・ ある時点において存在し、それ以降は改ざんされていないことを証明
 - 例) タイムスタンプ
各センサから出されるデータには、TaaSを活用してタイムスタンプを付与

(ii)信頼性の確保に必要なトラストのレベルに応じたトラストモデル

上記(1)で記載した機器から出るデータの信頼性の確保に必要な②の「機器」の信頼性の確保、トラストの確保の仕組みについては、3. 実現方法のところではトラストの分類を(1)プライベートトラスト、(2)パブリックトラストと2つに分類したが、(1)のプライベートトラストは、さらに組織内か、組織間か、また船舶、医療などの業界団体(参加、脱退の手続きがある)というようなコミュニティレベルで確保するかどうかで分類が分かれ、パブリックトラストを含めて下記4つのタイプでの実現が考えられる。

(ア)ローカルプライベートトラスト

自社で製造した製品を自社の認証局が発行する証明書によりトラストを確保

(イ)ピアトラスト

製品を製造する事業者と製品を使う事業者との二者間でトラストを確保

(ウ)コミュニティトラスト

製品を製造する社が所属する業界団体等のコミュニティからの証明書により
トラストを確保

(エ)パブリックトラスト

公的な機関の証明書によりトラストを確保

以下に信頼性の確保する(事例1)(事例2)を示す。

(事例1)(ア)ローカルプライベートトラスト&(イ)ピアトラストの活用事例

現状は、多くの機関で自社の認証局を活用している。製造業者 A が運用する自社の認証局（以下、プライベート CA）を利用することで、遠隔監視やリモートメンテナンスのトラストを向上するユースケースを示す。製造業者 A のプライベート CA は、プライベート CA の証明書と対応する秘密鍵を保持しており、アクティベート用証明書とサービス用証明書(製品が提供するサービスで生じたデータに付されるデジタル署名を検証するための証明書)を発行できるとする。発行手順を以下に示す。

1. 製造業者 A は、製造プロセス等が信頼できるサプライヤから調達した部品を用いて、製品 A'を製造する。
2. 製造業者 A は、プライベート CA が発行したアクティベーション用証明書(製品の機能を有効化する際のライセンス認証に用いられる証明書)と対応する秘密鍵を、製品 A'に組み込む。
3. 製造業者 A は、製品 A'を事業者 B に設置し、プライベート CA 証明書とアクティベーション証明書を用いたアクティベート処理を行う。アクティベート処理に成功した場合、プライベート CA が発行した製品 A'にはサービス用証明書と対応する秘密鍵が組み込まれる。
4. 製品 A'は、イベント・ログ・アラートなどの自身の出力データに対して、サービス用証明書に対応する秘密鍵でデジタル署名を付し、製造業者 A に送信する。
5. 製造業者 A は、製品 A'に割り当てられたサービス用証明書を用いて、出力データに付されたデジタル署名を検証する。デジタル署名の検証に合格した場合、出力データは信頼できるものとして受理し、リモートメンテナンスサービスに利用する。検証に不合格の場合は、出力データは信頼できないものとし、リモートメンテナンスサービスに利用せず、信頼できない出力データを受理したログを記録する。

プライベートトラストのみが成り立つ場合は、事業者 B は製造業者 A のプライベート CA が発行する証明書を信頼していないことを意味する。そのため、上述の方法では、事業者 B がデータの信頼性を技術的に検証できないという課題がある。しかし、製造業者 A が、自身が製造した製品の保守等を行う目的に限定すると、十分な信頼性

が確保できているといえる。

ピアトラストが成り立つ場合は、事業者 B は製造業者 A のプライベート CA が発行する証明書を信頼することができる。そのため、上述の方法で、事業者 B も製品とデータの信頼性を技術的に検証することができる。しかし、プライベート CA が信頼できるものであることを確認するために、個別の検証や契約等が必要となる。

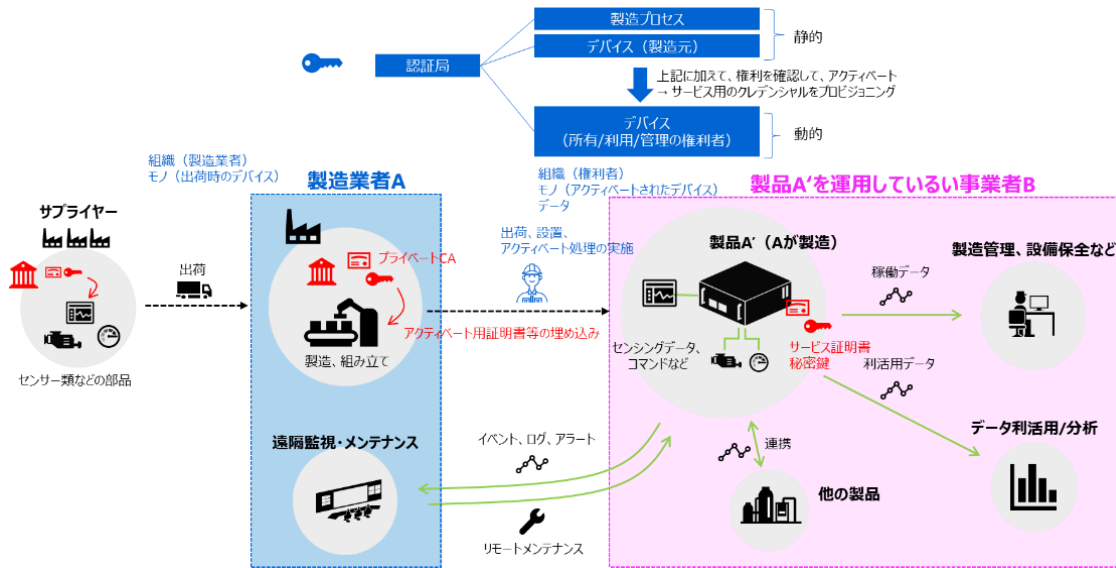


図 V-7 ピアトラストの活用事例(現状)

また、データの生成プロセスの確からしさを追加で検証することにより、データそのものの正しさも示すことが可能となり、保守メンテナンスサービスの品質向上に貢献可能である。

(事例 2)パブリックトラストの活用事例

将来的にはサードパーティーのトラストサービスを活用する事例も出てくることが期待される。製造業者 A が運用する中間 CA を利用することで、遠隔監視やリモートメンテナンスのトラストを向上するユースケースを示す。製造業者 A はルート CA から中間 CA の証明書と対応する秘密鍵を割り当てられており、アクティベーション用証明書とサービス用証明書を発行できるとする。発行手順を以下に示す。

1. 製造業者 A は、製造プロセス等が信頼できるサプライヤから調達した部品を用いて、製品 A'を製造する。
2. 製造業者 A は、中間 CA が発行したアクティベーション用証明書と対応する秘密鍵を、製品 A'に組み込む。
3. 製造業者 A は、製品 A'を事業者 B に設置し、ルート CA 証明書、中間 CA 証明書、

アクティベーション用証明書を用いたアクティベート処理を行う。アクティベート処理に成功した場合、プライベート CA が発行した製品 A'にはサービス用証明書と対応する秘密鍵が組み込まれる。

4. 製品 A'は、イベント・ログ・アラートなどの自身の出力データに対して、サービス用証明書に対応する秘密鍵でデジタル署名を付し、製造業者 A に送信する。
5. 製造業者 A は、製品 A'に割り当てられたサービス用証明書を用いて、出力データに付与されたデジタル署名を検証する。デジタル署名の検証に合格した場合、出力データは信頼できるものとして受理し、リモートメンテナンスサービスに利用する。検証に不合格の場合は、出力データは信頼できないものとし、リモートメンテナンスサービスに利用せず、信頼できない出力データを受理したログを記録する。

業界団体などのコミュニティ内のトラストが成り立っている場合は、製造業者 A と事業者 B が同じコミュニティに属していれば、ルート CA を介して、製造業者 B は製造業者 A が運用する中間 CA を信頼できる。

さらに、パブリックトラストが成り立っている場合は、製造業者 A と事業者 B が同じコミュニティに属していない場合でも、ルート CA を介して、製造業者 B は製造業者 A が運用する中間 CA を信頼できる。そのため、製品・データを用いたサービスへの障壁が下がり、新たなサービスの出現を促すと期待できる。

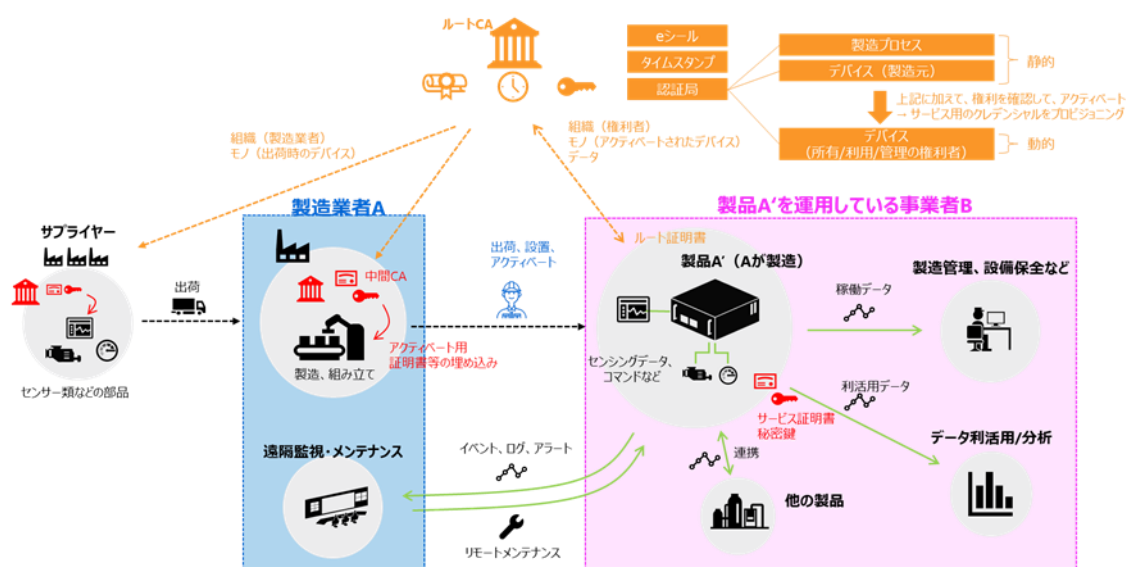


図 V-8 パブリックトラストの活用事例

(ア)、(イ)、(ウ)、(エ)どのタイプのトラストモデルを使うかは、ビジネスタイプ、事業者の事業規模、事業分野により求められるトラストのレベルが異なるため、柔軟な対応が求められる。

また、上記(事例1)、(事例2)の(i)-(ア)機器の利用者(組織)が正しいこと(事業者A、Bの組織の証明)については、ルートCA等から事業者Bに発行されたeシールの活用(eシール用電子証明書の拡張領域に記載する)や、タイムスタンプの活用が考えられる。また、(i)-(ウ)「存在・時刻」機器から生成されたデータの時刻が正しいことについても同様である。一方で、事業者A、Bがeシールやタイムスタンプなどの外部(第三者)のトラストサービス(TaaSを構成する要素の一つであるトラストサービス)の活用を促す制度の整備、CAの認証局の運営費の補助などのインセンティブの検討が必要である。さらに、中小企業などプライベートCAの設立が困難なところが、この仕組みから取り残されないように既にピアトラストで実現している事業者の枠組みに入るなど、様々な方策の検討が必要である。

以上の実現方法を用いれば、製品からのデータの示す機器が、実際に存在することや、詐称していないことを容易に確認でき、保守メンテナンスサービスのタイミングを診断する際に用いることができる。また、データの生成プロセスの確からしさを追加で検証することにより、データそのものの正しさも示すことが可能となり、保守メンテナンスサービスの品質向上に貢献可能である。

4-2. サプライチェーン全体で二酸化炭素排出量を減らす取り組み

トラストの概要

本ユースケースは、車両メーカーを例とするようなサプライチェーンにおける二酸化炭素排出量をゼロにする取り組みを社会に示すため、製品のサプライチェーン全体での二酸化炭素排出量の算定結果を説明する場合を取り上げる。

地球温暖化対策のため企業には脱炭素化を進めることが社会的な責務となっている。二酸化炭素排出量は、GHG プロトコル(Green House Gas Protocol)¹⁵にて、図 V-9 に示すようにサプライチェーン排出量が Scope 1 (直接排出)、Scope 2 (間接排出)、Scope 3 (Scope1, 2 以外の図 V-9 中①～⑮での排出)で定義されている。排出量は活動量と排出原単位を掛け合わせて算定される。活動量は事業者の活動の規模に関する量、例えば、Scope1 の自社での燃料の燃焼や Scope2 の自社での電気の使用量、Scope3 の貨物の輸送量や廃棄物の処理量などが該当する。自社の燃料や電気の使用量であれば、燃料や電力の消費量を測定すればよいが、他社での貨物の輸送、配送に関わる活動量となると輸送トラックの燃費や積載量も含めて把握が必要となり、それらの活動量の値とともにその算定過程を確認しなければならない。

こうした排出量の算定に関して、欧州では製品ライフサイクルを通じた環境負荷を評価するライフサイクルアセスメント LCA 規制¹⁶と呼ばれる動きがあり、欧州で事業する事業者は、第三者認証も含めて対応が必要となることが想定される。

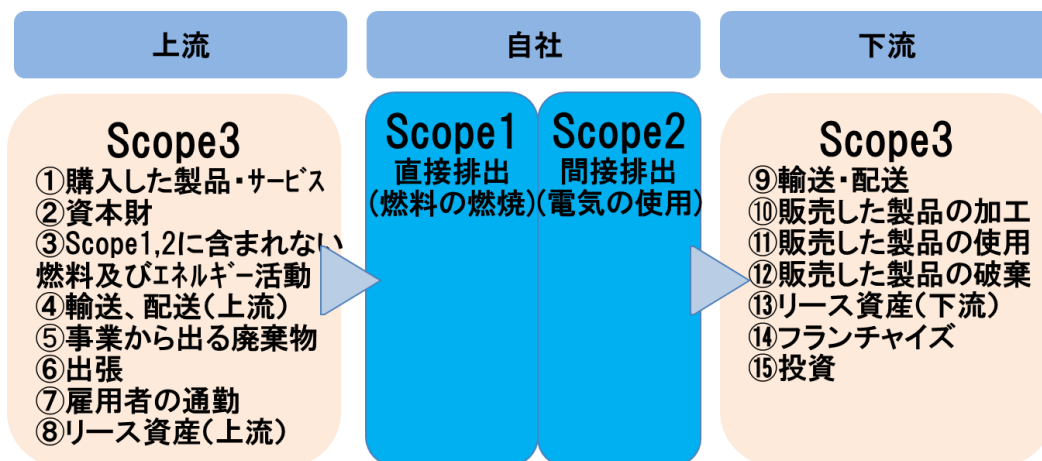


図 V-9 サプライチェーンでの排出量の Scope1, 2, 3 の分類([環境省サプライチェーン排出量算定]より図を引用)

¹⁵ Greenhouse Gas Protocol, URL=<https://ghgprotocol.org/>

¹⁶ European Platform on Life Cycle Assessment (LCA),
URL=<https://ec.europa.eu/environment/ipp/lca.htm>

Before(課題)

環境省のガイドライン¹⁷によると、活動量の把握には従来のサプライチェーンの活動量に加えて、排出量の算定に特有な、例えば Scope3 における貨物の輸送量や廃棄物の処理量といった活動量まで把握しなければならず、時間や工数がかかる。今後こうした排出量の算定のプロセスには、LCA 規制などで第三者認証や、排出量の値の正確性が従来以上に求められることも想定される。これらの対応のため、事業者が排出量を正確に算定し、サプライチェーン全体での排出量の算定を第三者が根拠をもって確認しなければならず、算定プロセスに時間や工数がかかる。もし算定に使うデータの測定方法、条件、データの改ざんなどが一部でも疑われてしまうと、実態を把握し説明することが困難となる。

After(めざす姿)

サプライチェーンを構成する組織は、二酸化炭素排出量を算定するための活動量の把握に関わるプロセスを規程として定め、その規程どおりに行ったという実施記録を残すことで、以下のことが実現可能となる。

- ・実施記録を集めることで活動量の算定過程が信頼できることを容易に確認できる
- ・実施記録への改ざんの有無を検証できるように管理できる
- ・サプライチェーン全体での二酸化炭素排出量算定のプロセスの妥当性を、根拠をもって容易にリモートで説明でき、第三者認証にも対応できる
- ・活動量について求められる信頼度のレベルに応じて、プロセスとその実施記録の確認だけでなく、測定機器の検証や測定、データの検証を可能とする仕組みを導入することで、より高い信頼性を確保することができる

実現方法

サプライチェーンを構成する組織は、サプライチェーン全体での二酸化炭素排出量を算定するために、活動量に関わるプロセスを規程として定め、規程どおりに実施していることをデジタルエビデンスとして記録し、その記録を自社内で確認できるようにする。加えて、規程どおりに実施したという記録が意図的に改ざんされることや過失により変更されても、あとで検出できるようにする(要件1)。

サプライヤから廃棄業者までの個々の部材や部品、モジュール、製品の製造過程や運用過程、廃棄過程を規程として予め定め、規程に基づいた実施記録と、その実施記

¹⁷ 環境省グリーン・バリューチェーンプラットフォーム：サプライチェーン排出量算定をはじめの方へ (env.go.jp)

http://www.env.go.jp/earth/ondanka/supply_chain/gvc/supply_chain.html

録から活動量を算定する。規程と規程に基づいた実施記録を照らし合わせて、実施記録が妥当であることの実施確認を行い、図 V-10 に示すようにその結果とともに活動量から算定した二酸化炭素排出量をトラストストアに記録する。例えば、車両モジュールメーカーが ECU(Electronic Control Unit)を製造する場合、部品メーカーから購入した MCU(Micro Controller Unit)やメモリなどの部品を使った製造工程を、モジュール製造規程として予め定める。さらにそのモジュール製造規程の中で、各種の活動量の予測も予め定め、モジュール製造実施記録に活動量実績も記録する。このモジュール製造規程とモジュール製造実施記録とを照らし合わせることで、その規程に基づく実施内容が妥当であることの実施確認を行い、活動量に排出原単位を乗じて算定した二酸化炭素排出量を算定し、トラストストアに記録する。サプライチェーンを構成する部材メーカー、部品メーカー、車両モジュールメーカー、車両メーカー、車両ユーザ、廃棄業者が、図 V-11 に示すようにデジタルエビデンスを基に算定した二酸化炭素排出量をトラストストアに記録し、サプライチェーン全体で共有する。サプライチェーンを構成する組織は、サプライチェーン全体で算定した二酸化炭素排出量を共有することにより、部材や部品、モジュール、車両製品の製造過程や運用過程、廃棄過程の二酸化炭素排出量とその算定過程が信頼できることをリモートで容易に確認できる(要件 2)。

車両の部材や部品やモジュールの供給ルートのみならず、配送ルートや運用箇所、さらには車両の破棄までを辿れるよう、図 V-11 に示すようにトラストストアでサプライチェーンを構成する組織を辿る紐づけ情報を付加する。トラストストアでの紐づけ情報により、例えば、部材メーカーから廃棄業者までを辿って、Scope 1, 2 のみならず、Scope 3 の二酸化炭素排出量とその算定過程が信頼できることをリモートで容易に確認することができる(要件 3)。

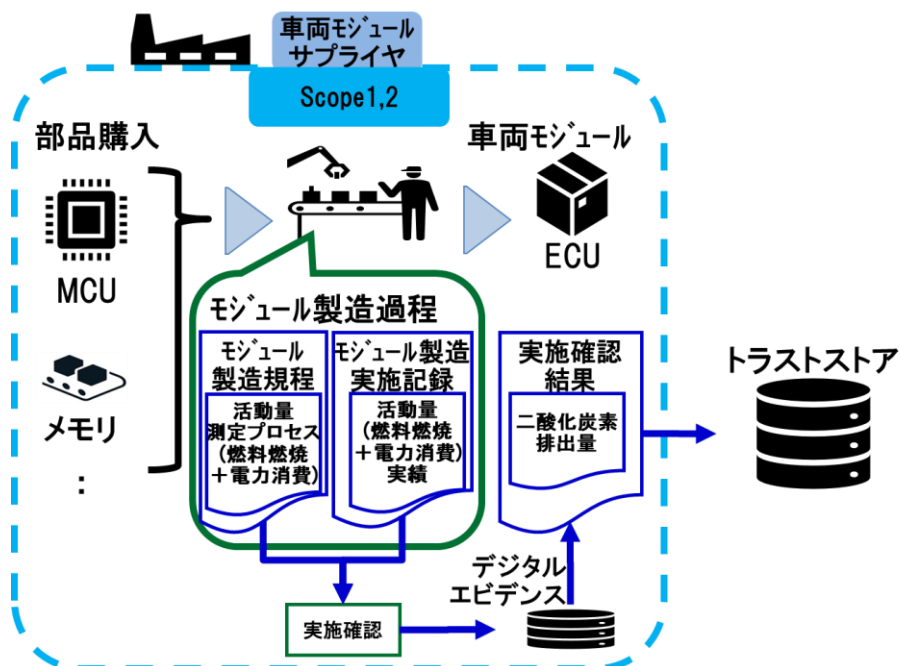


図 V-10 信頼性を示す情報のトラストストアへの格納

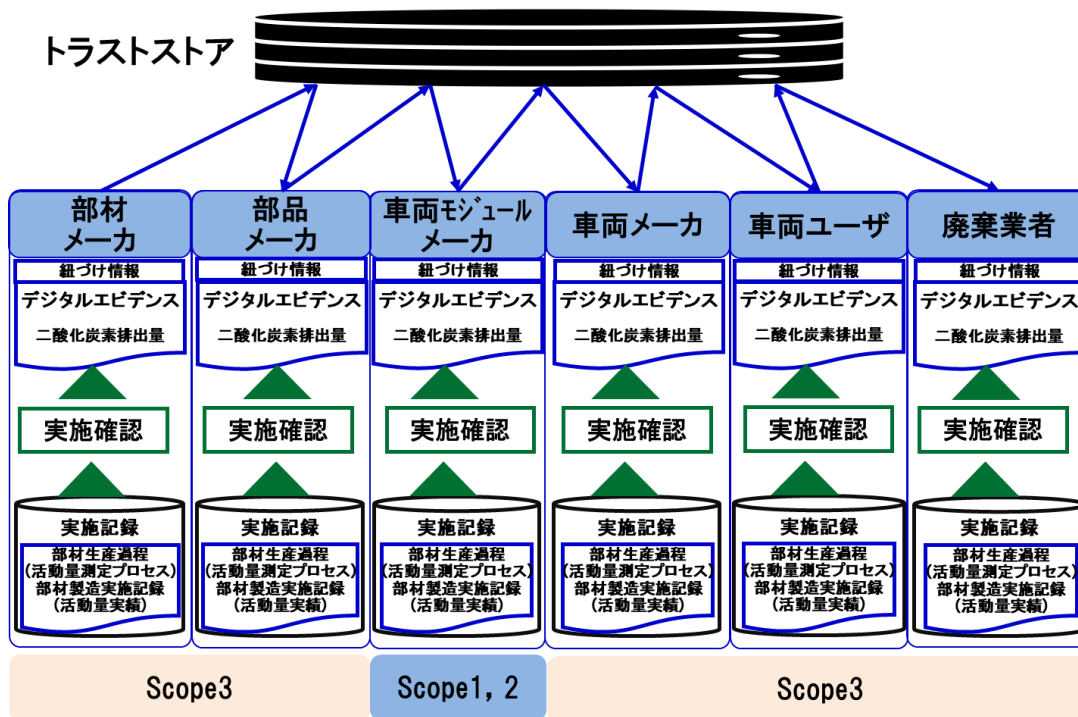


図 V-11 サプライチェーン全体での二酸化炭素排出量管理

また、サプライチェーンを構成する組織に、事業形態や適用ケースに求められる信頼性のレベルや規制が求める信頼性のレベルに応じてより高い信頼性が要求されるケ

ースが予想される。

例えば、活動量の把握において、人間が目視などで収集したデータを基に算出するよりも、信頼できるセンサを用いて計測したデジタルデータの方が、人為的なミスなどが混入しないという意味で、信頼性が高いといえる。さらに、センサを用いて計測した「活動量」(データ)自体が改ざんされていないことの保証を行うことで、さらに信頼性を高めることができる。

すなわち、ユースケース(4-1 項)で示した「機器から出るデータの信頼性を確保する仕組み」や、センサが出力した数値を信頼する基準を定め、「活動量の数値」を保証する仕組みが確認できると、信頼性がさらに向上できる。このような保証の仕組みは、TaaS を活用することで、容易かつ安価に実現できるようになる。そして、サプライチェーンの性質に応じて、適切な手段、信頼性のレベルが選択できることが望ましい。

4-3. 製造サプライチェーン全体のセキュリティ対策の確認

トラストの概要

本ユースケースは、製造サプライチェーン全体のセキュリティを確認する事例である。サプライチェーンを構成する組織は製品提供先との契約に基づき、契約どおりの品質と納期、価格（いわゆる QCD）で製品を納入する義務を負う。加えて QCD 以外の契約条項として、例えば、製品の製造過程におけるセキュリティ対策を、サプライチェーンを構成する組織は実施することが要求される。

自動車製造業において、例えばドイツの自動車メーカーは、製造サプライチェーンを構成する組織に対して、試作車両の設計情報が委託先から漏洩しないようなセキュリティ対策を求めている。

Before(課題)

製造サプライチェーンを構成する組織が製造過程でセキュリティ対策を実施していることを確認するには、製造規程とその規程に基づいて実施された内容を照らし合わせる必要があり、セキュリティ対策が妥当であることの確認に多くの時間や工数がかかる。そして、製造サプライチェーン全体で実施するセキュリティ対策が妥当であることを確認するには、さらに多くの時間や工数がかかる。

After(めざす姿)

製造サプライチェーンを構成する組織で実施すべきセキュリティに関わるプロセスを規程として定め、その規程どおりに実施したという記録を残し、その記録を集めることでセキュリティ対策が規程どおりに実施されたことを容易に確認できる。さらに、実施結果の記録を、記録された時点から改ざんの有無をあとで検証できるように管理する。これにより、製造サプライチェーン全体で実施するセキュリティ対策が規程どおりに実施されたことを時間や工数をかけずにリモートで容易に確認できる。

実現方法

製造サプライチェーンを構成する組織が製品の製造過程でのセキュリティに関わるプロセスを規程として定め、その規程に基づいて実施した内容もデジタルエビデンスとして記録し、その記録を社内を確認可能にする。加えて、規程どおりに実施したという記録が意図的に改ざんされたり、過失により変更されたりしても、あとで検証できるようにする(要件1)。

これらの規程と実施の記録を照らし合わせることで、製造過程のセキュリティ対策が規程どおりに実施されたことを確認し、その確認結果をトラストストアにてサプライチェーン全体で共有する。トラストストアに照会することで、時間や工数をかけずに

リモートで容易に確認することができる。

例えば、図 V-12 に示すように予め決められた車両モジュールメーカーの製造規程に含まれるセキュリティ規程と、モジュール製造実施記録にあるセキュリティ実施記録とを照らし合わせ、規程どおり実施されたことを確認する。その確認結果を、図 V-13 に示すようにトラストストアに記録し、車両メーカーと共有する。トラストストアに記録された内容を車両モジュールメーカーと車両メーカーとで共有することにより、車両メーカーは車両モジュールメーカー製品の製造過程のセキュリティ対策が規程どおり実施されたことを時間や工数をかけずにリモートで容易に確認することができる。(要件 2)。

製品の供給ルートや提供ルートを把握するために、図 V-13 に示すようにトラストストアで組織を辿るための紐づけ情報を付加する。トラストストアでの紐づけ情報により、例えば、製品の供給ルートや提供ルートにおいて、部材メーカーから車両モジュールメーカーまでを辿れるようにする。車両メーカーが供給を受ける車両モジュールメーカーの製造過程のみならず、より上流の部材や部品サプライヤでも、製造過程のセキュリティ対策が規程どおり実施されたことをリモートで容易に確認することができる(要件 3)。

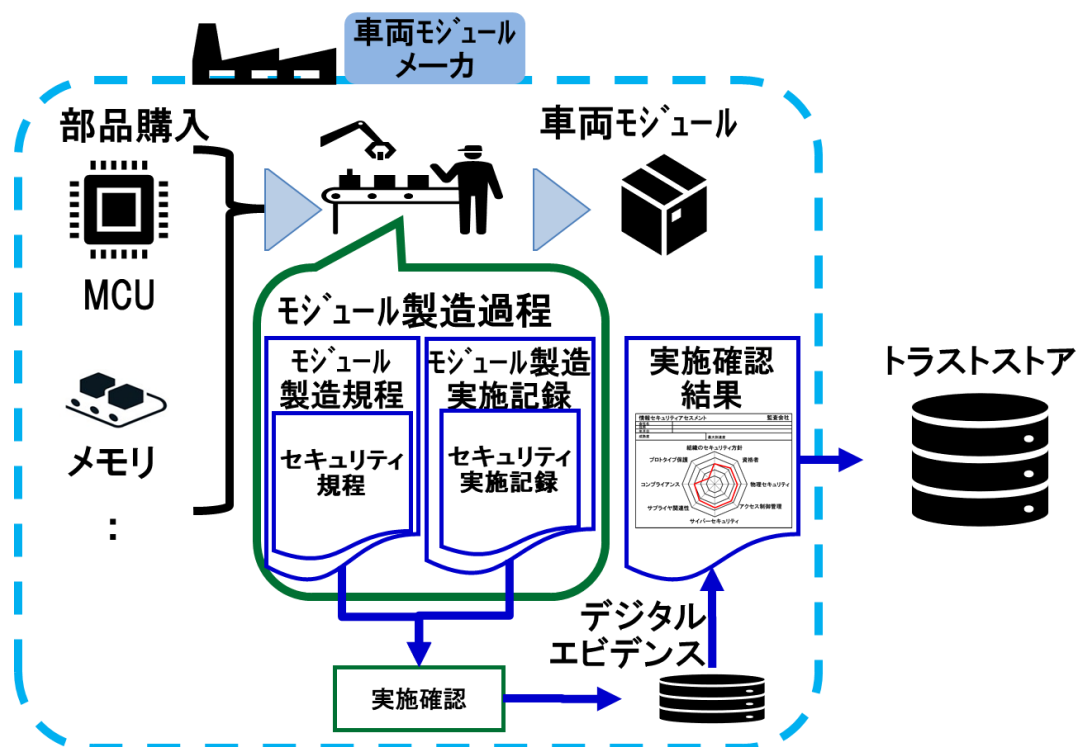


図 V-12 信頼性を示す情報のトラストストアへの格納

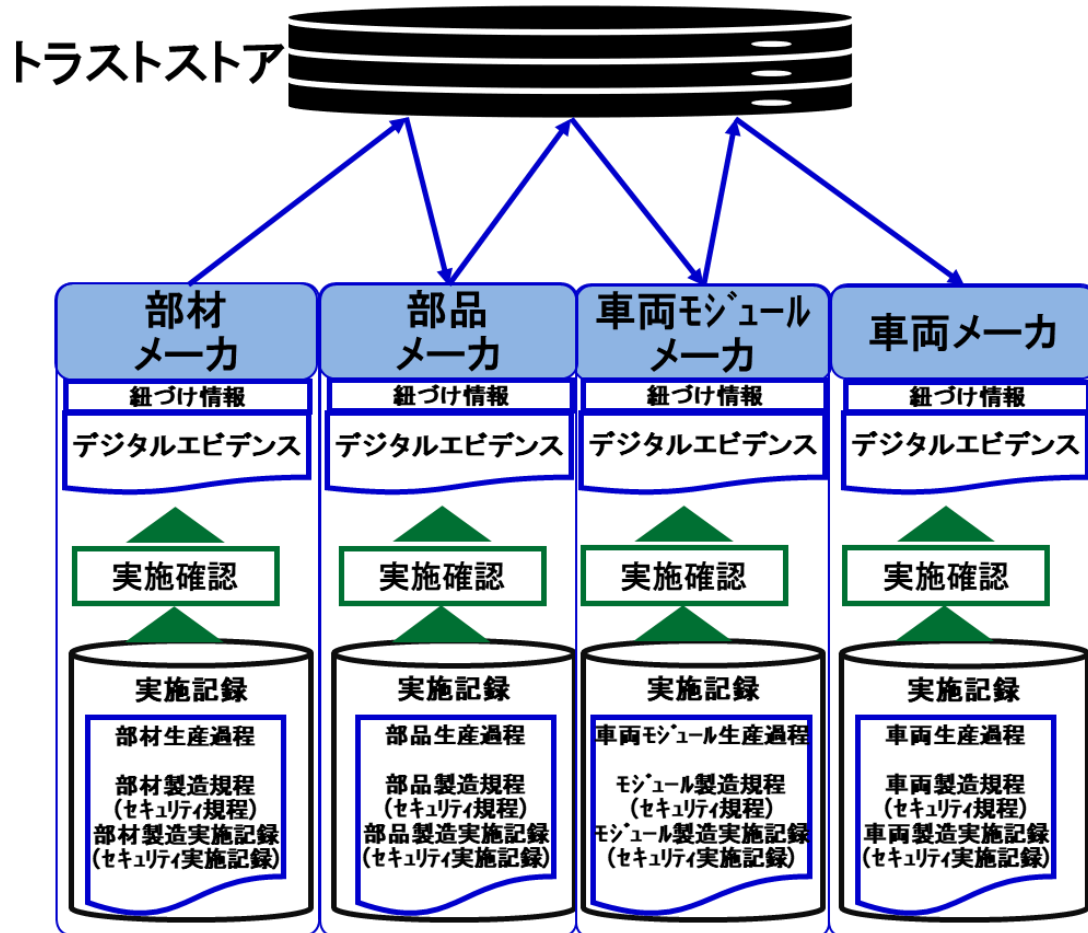


図 V-13 製造サプライチェーン全体でのセキュリティ対策管理

5. TaaS(Trust as a Service)の利用シーン・効果

TaaSがあることによるユースケース(4-2項)での効果を表 V 2 に示す。

表 V-2 TaaSがあることによるユースケース(4-2項)での効果

TaaSの役割	ユースケース(4-2項)での利用シーン(Scope3)	効果
送受信先確認	二酸化炭素排出量データのトラストストアへの登録時に、登録した企業を確認するために活用	当該企業が調達契約・インボイス(明細書、請求書、納品書)を発行した企業と同一であることがわかる
リモート型データ完全性(電子署名・リモート署名)	二酸化炭素排出量データとその確認結果をトラストストアに記録する際に活用	記録した後、データが書き換えられていないことがわかる
プロシージャ・システムの正当性(電子署名・リモート署名・タイムスタンプ)	製造サプライチェーンにおける活動量測定プロセスと、そのプロセスに基づく活動量実績の確認をする際に活用	二酸化炭素排出量算定に使う他社の活動量実績が正しいプロセスに基づいて算定されたことと、サプライチェーンでの活動の順番を辿れる
検証	トラストストアに記録された二酸化炭素排出量データを、サプライチェーンを構成する組織が確認する際に活用	二酸化炭素排出量の第三者による確認結果を他の第三者が再利用できる
利用者負担軽減(導入・運用容易性)	活動量測定プロセスを担うシステムを構築する際に活用	サプライチェーン上の様々な現場、工程のSEにとって、デジタル署名や署名検証の専門知識がなくても、時間・工数を少なく、活動量測定プロセスの構築ができる

トラストサービスはデータの内容そのものが正しいかどうかを担保するものではなく、データを発出する人、モノ、組織、が真正であり、発出後のデータの非改ざん性、自己が発出したデータであることを否認できないことを担保するものである。データ自身の内容が正しいのか推定する上ではその発出元となる人、モノ、組織、プロシージャ、システムの属性やコンテキスト情報を目的に応じて示すことにより発出元の信頼性の評価を容易とすることが重要となると考えられる。例えば、データ生成時に実際と異なるデータを故意に作成してトラストサービスで保護しても、データ利用者にはデータの内容が不正なものなのか分からないが、正しいプロシージャによるチェック機構を経て発出することにより、データに対する不正な操作を防止できる。データの内容が正しいことを評価するにはそのような別の手段が必要である。V-3節の実現方法に示したデジタルエビデンスやトラ

ストストアはその方法のひとつである。そのような属性証明サービスを従来のトラストサービスと組み合わせ、TaaSとして一体的に提供できるプラットフォームの検討も望まれる。

VI. 提言

サプライチェーンのトラストを実現する仕組みが、広く社会に利用されるようになるために、さまざまなステークホルダとの合意形成や普及の観点で提言を述べる。

提言. サプライチェーンのトラスト実現に向けた合意形成と国際的整合性の確保

- ・ 社会がサプライチェーンに求めることとして、SDGs や ESG など社会、環境への貢献や、グローバルに形成される規制・ルールを遵守していることなどが挙げられる。社会からの期待、要求に応えるために、以下の点を具体化する場を設置し、業界団体として合意を得るなどの取り組みを積極的に進めるべきである。
 - サプライチェーンを構成する組織全体に課せられる規程や、どこまで実施すれば良いかを判断するための基準やガイドライン
 - 業界、事業形態に応じて必要とされる信頼性のレベルやトラスト形成に関する考え方
 - サプライチェーン上でやりとりされるデータの信頼性を第三者に示すための基準やガイドライン
 - 機器から出るデータの信頼性を確保するための基準やガイドライン
 - プライベートトラストを円滑に確立するための基準やガイドライン
- ・ 製造過程やサービス提供過程のサプライチェーンがグローバルに広がっていることを考慮すると、本ホワイトペーパー「V 解決に向けた方策」で示した3つの要件、トラスト形成や確認に関する取り決め、考え方は将来的に国際的に通用するものでなくてはならない。そのため、関連する標準化団体や産業 IoT に関わる業界団体などに対し、国際的な整合性を確保していくことを日本が主導すべきである。

提言. サプライチェーンのトラストの普及、エコシステム形成に向けた制度面での支援

- ・ サプライチェーンのトラストを実現するには、サプライチェーンを構成する組織、特に中小企業にとってコスト増になる。さらに、一部の組織のみが導入してもサプライチェーン全体のトラストは実現されない。これらの課題を解決するには、コストに見合う効果や、サプライチェーンを構成する組織全体で取り組むインセンティブの具体化が必要になる。

また、トラストを持続させるには、実現の仕組みを最新化し、継続的に運用されることが必要である。具体的には、サプライチェーンを構成する組織が自ら投資して、それを上回る効果を得て、それぞれの事業を成長させる、というエコシステムの形成が重要になる。

こうしたインセンティブの具体化やエコシステムの形成に向けて、短期、中長期的にそれぞれ制度面でどのような支援、施策が可能であるかを検討し、具体的なマイルストーンとロードマップを議論、策定する場を設けるべきである。

- ・ サプライチェーン全体での取り組みを実現するにあたって、サプライチェーンを構成するさまざまな組織、業界を跨った場合の技術的な実現性、整合性の検討が必要であり、サプライチェーンのトラストの価値・効果を具現化する必要がある。そのために、各種機能のリファレンス実装を行い、さまざまな業界が協調して技術や価値の検証、実証を通じた実用化を行っていく場を設ける必要がある。

VII. おわりに

サプライチェーンのトラストを実現するために、今後は、ユースケース、対象業界を定め、本ホワイトペーパーの内容、技術仕様をより具体化していく必要がある。

- ・ 規程、期待の共通的な記述方法や実施確認内容
- ・ 信頼性の評価や信頼のリスクをどこまで許容するかを評価するための情報
- ・ トラストストア、デジタルエビデンスの利活用インタフェース仕様
- ・ 複数のトラストストアが連携して機能するためのトラストストア間の連携インタフェース仕様
- ・ TaaS、ベース・レジストリを含めた全体の連携技術
- ・ 機器の ID 管理手法も含めた、機器用公開鍵証明書管理技術
- ・ 機器の安全な鍵管理技術

以上