Trusted Web の実現に向けたユースケース実証事業

成果報告書

Trusted Network による社会 IT インフラの信頼性・強靭性向上の実現

2023 年 3 月 24 日（提出日）

アラクサラネットワークス株式会社

目次

1　背景と目的 5
1.1 事業の背景 5
1.2 事業の目的 6
2　事業の概要 6
2.1　事業概要及び実証の範囲 6
2.1.1　事業概要 6
2.1.2　実証の範囲 8
2.2　社会・経済に与える価値・影響 15
2.2.1　ユースケースが解決しうる課題 16
2.2.2　IT 製品のトラスト向上ニーズ 17
2.2.3　政治・行政、企業活動・経済活動、社会、技術革新における課題の解決 18
2.3　コンソーシアムの体制 20
2.4　実証全体のスケジュール 21
3　実証内容 22
3.1　実証の実施事項、論点及び判断 22
3.1.1　Trusted Network プロジェクト 22
3.1.2　TN のめざすトラストと基本アーキテクチャ 24
3.1.3　プロトタイプの企画・開発 27
3.2　検証できる領域を拡大する仕組み 29
3.2.1　データフロー 29
3.2.2　データフローに登場する主体とその概要 34
3.2.3　検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容 35
3.2.4　本システムで形成を目指す合意とその履行のトレースの内容 39
3.3　6 構成要素との対応 42
3.3.1　検証可能なデータ 42
3.3.2　アイデンティティ 42
3.3.3　ノード 43
3.3.4　メッセージ 43
3.3.5　トランザクション 44
3.3.6　トランスポート 44

3.4　本実証で企画・開発したシステムの概要 45
3.4.1　動作シーケンス 45
3.4.2　業務フロー 53
3.4.3　ユースケース図 56
3.4.4　操作画面（UI） 60
3.4.5　機能一覧/非機能一覧 60
3.4.6　データモデル定義(VC データモデルを採用する場合) 69
3.4.7　実験環境 70
3.4.8　システムの構成要素 70
3.5　実証を通じて得られた主な成果 71
3.5.1　システムの企画・開発に関する実証内容・得られた主な成果 71
3.5.2　ビジネスモデルに関する実証内容・得られた成果 71
3.6　本実証で開発したシステムの第三者による再現可能性 72
4　実証終了後の社会実装に向けた見通し 73
4.1　社会実装時に想定しているビジネスモデル・ユーザーのメリット 73
4.2　実証を通じて判明したユースケースの課題とその解決方針 75
4.3　本ユースケースの社会実装に向けたマイルストーン 76
5　Trusted Web に関する考察 78
5.1　Trusted Web のアーキテクチャに関する課題と提言 78
5.1.1　実装アーキテクチャの具体化 78
5.1.2　検証性に関する方針の明確化 79
5.2　その他 Trusted Web の課題と提言 79
5.2.1　ビジネス 79
5.2.2　政策とグローバリゼーション 80
付録 A.　TNP が管理する情報とその属性 82

用語集

用語	定義
CDM	Continuous Diagnostics and Mitigation。米国連邦政府機関のセキュリティを強化するための継続的な診断と脅威の緩和を行うプログラム。Trusted Network ではこれを企業向けに適用可能な仕組みに拡張した。
BOM, トラスト BOM TBOM	IT インフラを調達する者が必要とする製品信頼情報で、Trusted Network ではトラスト BOM（または TBOM）と呼ぶ。BOM は Bill of Materials の略。トラスト BOM にはハードウェアを構成する部品情報(ベンダ名、原産国、型番等)である HBOM、ソフトウェア情報（OSS, 基本ソフトの Ver.番号等）、設定情報、その他からなる SBOM がある。
GNS3	Graphical Network Simulator-3 は、2008 年に最初にリリースされたオープンソースのネットワークソフトウェアエミュレーター。
HBOM	Hardware Bill of Materials
IPFS	InterPlanetary File System P2P ネットワークで分散的に稼働するストレージサービス HTTP のような中央集権的なロケーション指向型プロトコルではなく、ネットワーク上のノードが分散してデータを管理しているコンテンツ指向型プロトコルを用いている。ロケーション指向型に比べて耐障害性、耐改ざん性負荷分散および耐検閲性に優れる。
NFT	Non-Fungible Token： 非代替性トークン ブロックチェーン技術を利用して替えが効かない唯一無二であることを証明する技術。
NIST	National Institute of Standards and Technology: 米国立標準技術研究所。1901 年に設立され、現在は米国商務省（Department of Commerce：DoC）の傘下の研究機関。セキュリティに関する研究と基準制定も行っている。
Root of Trust	信頼の証明書。規格・基準の順守度診断結果をデジタル証明書として信頼の起点とする。
SBOM	Software Bill of Materials
SCRM	Supply Chain Risk Management
Society 5.0	「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させ、経済発展と社会的発展を両立する人間中心の社会」（第五期科学技術基本計画）。
TNE	Trusted Network Enabler：Trusted Network に各種機能や技術を提供するパートナー企業・公共機関。

TNDP	Trusted Network Data Platform： 製品信頼情報やアセスメント結果に関する情報を格納するデータ基盤。ブロックチェーン基盤上に構築される。
TNP	Trusted Network Platform： Trusted Network を構成するシステム基盤全体。
TNSP	Trusted Network Service Provider：Trusted Network の運用主体。Trusted Network Platform を管理・運営する公益的第 3 者。
アセッサ（Assessor）	ベンダとインテグレータの企業としてのセキュリティ基準への適合状況のアセスメント、ベンダの製品のセキュリティ規準や製品信頼情報の開示レベル等のアセスメントを実施し、その結果を Trusted Network 利用者に開示することで、ベンダとインテグレータ、製品の優位性や法制および調達基準への適合性の根拠を提供する主体。ベンダ、インテグレータとの利害関係のない第 3 者がアセッサとなる。
アセッシ（Assessee）	アセッサからアセスメントを受ける主体。ベンダおよびインテグレータがアセッシとなる。
インテグレータ	ベンダから IT 製品を調達し、事業者ごとのシステムの企画から IT 製品の導入・構築・設定、保守、運用支援等の工程を担う業務を行う企業。 （同義語）システムインテグレータ、SIer
インフラ事業者	事業者のうち、社会基盤となるインフラを提供する企業あるいは組織 （同義語）重要インフラ事業者。
運用セキュリティ	サービスの運用において、サービスを構成する機器の脆弱性と機器へのサーバーセキュリティ攻撃及び不正アクセスを管理しデータを保全することで、サービスの安定と永続的な提供を確保するための仕組み。
エコシステム	企業や人が「群」として集まり、分散している場合よりも高い生産性を生むような「共創状態」や「共創の場」を指す。 「多様な構成員の相互協力および平等かつ透明な収益の循環が、エコシステムを健全に機能させる条件」となる。
機器真正性セキュリティ	機器を構成するハードウェアとソフトウェアに改ざんが無いことを担保するための仕組み。
コンソーシアム	ある目的に向かって企業などが集まり、資源の有効活用を図る閉鎖的な集合体。リーダー企業の構想力と参加企業の利害関係の統治力に依存。
サプライチェーン	製品やサービスを提供するために必要な要素を提供する供給網を指す
サプライチェーンセキュリティ	ベンダが製品（本書では IT 製品とする）を提供するために調達するハードウェア（部品）やソフトウェアのトレーサビリティを管理し改ざんを防止・保証するための仕組みや、インテグレータがシステム（本書では IT システムとする）を提供するために調達した製品のトレーサビリティを管理し改ざんを防止・保証するための仕組み、そして事業者がサービス（本書では主に通信や

	電力・水道・金融などの公共的サービスとする）を提供するために調達するシステムのトレーサビリティを管理し改ざんを防止・保証するための仕組み。
事業者	インテグレータから IT 機器を調達する IT 機器の利用者・組織
信頼情報	ある主体が提供するウ製品やサービスの信頼を担保するための客観的なデータやエビデンス（証跡）を指す。
脆弱性セキュリティ	機器に対する外部からのアク。セスや攻撃に関する脆弱性を管理し保証する仕組み
第三者アセスメント	製品やサービスを提供する当事者以外と利害関係を有しない第三者による、当事者に関する法律・ガイドライン遵守性や安全性などの監査行為を指す。
調達取引	ある組織（企業や政府など）がある目的（サービスの提供など）のために必要な機器やサービスを購買するための取引行為を指す。
デジタル ID	Trusted Network エコシステム参加主体に割り当てられるユニークな ID
トラスト（Trusted Network におけるトラストの定義）	概念的には、社会的価値及び経済的価値を持続的に創出する信用または信頼関係を示す。 具現的には、主体が資産に関連する様々なリスクへの対応に取組み、見える化することで、取引において、他者から見て安心できるレベルの状態であることを示す。様々なリスクとは、地政学的リスク、環境的リスク、経済的リスク、技術的リスク、コンプライアンスリスク、サイバーリスク、評判・風評リスク等を指す。 トラストを構成する技術や仕組みが透明かつオープンであること・トラストを提供する主体がトラストを客観的に証明できること・トラストの提供を受ける主体がトラストを客観的に検証できること・中立的な第三者がアセッサになれること、等の条件が必要となる。
トラストアンカー	デジタル資産化されたベンダ・製品・インテグレータのアセスメント結果に付帯される、トラストの起点となる証明書／エビデンス。あるいはそれを提供する主体（アセッサ）を指す。
トラスト保守サービス	ベンダ（あるいはベンダから支援を受けたインテグレータ）が事業者に対して、Trust BOM を提供、更新をサポートするとともに、Trust BOM を最新の状態に維持することで、真正性や脆弱性の有無を常に把握できるようにするサービス。
ベンダ	IT ハードウェア（機器）またはソフトウェア製品を提供するメーカー。 製品の設計／開発／製造は自社で行う場合と、他社に委託する場合がある。

経済安全保障推進法	正式名称は、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」。2022 年 5 月に成立。
重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、 わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの。 経済安全保障推進法では、重要インフラ事業者に相当する特定社会基盤事業者として電気、ガス、石油、水道、鉄道、貨物自動車輸送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカードの 14 分野を指定。
製品信頼情報	Trust BOM、トラスト BOM、TBOM
論理 NFT	Trusted Network 上で IT 機器に対する契約や所有状況を表す NFT。契約締結によって所有者が変わり、所有者の履歴情報が管理される。

1　背景と目的

1.1 事業の背景

IT インフラ調達と運用におけるサプライチェーンセキュリティ・機器真正性セキュリティ・運用セキュリティ（含む脆弱性セキュリティ）の向上は、経済安全保障推進法の施行に見られるように、日本として国家的取り組みが求められる社会課題となっている。

日本での今日の IT インフラの調達取引において、上記要素の基礎的な検証性を提供するシステムがオープンかつ網羅的に提供されているとは言えず、各事業者の独自かつ個別な情報収集や取り組みによって個々のベンダやインテグレータを信頼することで取引が成立、即ち合意形成されているのが実態である。事業者個別の情報収集には事業者個別にコストが発生し、ベンダやインテグレータの情報提供にも個別のコストが発生することから、国家的に多大な経済的分割損をもたらすとともに、ベンダやインテグレータで発生したコストが事業者に転嫁され事業者負担が増大しやすい構造から、事業者の利益と成長の確保や利用者負担とのトレードオフにより十分な網羅性や客観性が担保されないリスクを有している。資本主義経済の原則に照らし合わせて考えれば、これらの活動がもたらす信頼性の差異化による競争性が堅持されているという観点では健全性が高いが、一方で個々のステークホルダのコスト負担能力や投資判断への IT インフラ信頼性の依存性の上昇やバラつき、規模の経済の大企業偏重化の進行など、日本全体の IT インフラ信頼性や経済最適化の観点では懸念すべき事柄も共存している。

更に、サプライチェーンの拡大による全体系の複雑化・不透明化・予測困難化は日々進行しており、各事業者とベンダ・インテグレータの間で成立する個別の信頼をベースにした合意形成が成長と革新の阻害要因となり、国民生活の安全や国際競争力の確保するのが困難になりつつあるという実態にも何らかの打ち手が必要と考えた。

IT インフラの信頼性向上という公益的な社会課題解決ユースケースの性質より、システム利用者が主体的にデータと取引をコントロールしトレースできること、システムが主体間の競争や取引の自由を制限しないこと、が現在のサプライチェーンの商流に適用するための絶対的な要件となる。そのうえで、社会的に最低限必要な共通項を括りだして管理することで、ベアミニマムコストの分割損やバラつきや経済偏重性を解消し、インフラの信頼性向上のみならず新しい経済モデルによる経済の活性化と発展を実現できると考えた。

1.2 事業の目的

社会インフラ事業者を中心とした企業、官公庁・自治体・公共機関が IT 機器を調達・運用する際、[1]当該製品のサプライチェーンセキュリティへの取り組みに関する十分性（第三者アセスメント結果）の検証、[2]当該製品の信頼情報とトレーサビリティの検証、[3] 当該信頼情報の透明性と十分性及び提供者による主体的な root of trust（信頼の証明書）の有無に関する検証、[3]当該製品と当該信頼情報の真正性（唯一無二かつ改ざんされていないこと）の検証、[4]当該製品の永続的な信頼性の検証、を提供することで、調達取引において客観的な合意形成の履行を実現し、社会インフラの信頼性向上に貢献する。

2 事業の概要

2.1 事業概要及び実証の範囲

2.1.1 事業概要

上記の背景を踏まえ、事業目的を達成するために、当社は「Trusted Network」（TN と略記） という IT 機器の真正性情報を安全に共有するネットワーク基盤を独自に創出した。TN の基本要件は、Trusted Web の基本要件と合っており、本事業では Trusted Web の利活用を前提としたユースケースの実現方法や実現要件を企画する。

TN は、事業者の IT 機器調達において、サプライチェーンリスク管理の十分性、製品構成と履歴の透明性・トレーサビリティとその網羅性、情報の信頼証明性、脆弱性・真正性の持続的管理性等に関する検証性とその領域を拡大することで、取引の客観的合意形成と実績の管理を実現し、社会インフラ信頼性・強靭性向上を実現する。

本実証事業では、事業者（基幹インフラ事業者を含む IT インフラ調達者）にベンダがインテグレータを通して IT 製品の製品信頼情報（Trusted Bill of Materials、省略形で TBOM と呼ぶ）を安全に提供し、事業者が TBOM を利用することで IT インフラの調達と運用において IT インフラの継続的な信頼性（Trustability）の検証を可能とするネットワーク基盤 Trusted Network を Trusted Web のユースケースとして実証する。

製品信頼情報は製品のハードウェアやソフトウェアの構成など機微な情報を含むため、この情報が改ざん又は漏洩される事無く流通できる基盤を準備し、データ提供者による Roof of Trust の提供も実現する。本報告書の 1 章で述べた通り、このような合意形成を実現するためには無視できないコストが発生し、更に合意形成の検証と信頼性が事業者のナレッジベースに依存する傾向があるが、TN の提供により既に一部顕在化している社会課題を業種や事業者、ベンダやインテグレータ横断でワンストップに解消できる。

TN は、エコシステム（収益活動協調体制）で形成される。TN には、ベンダ、インテグレータ、事業者という IT 機器の取引・調達に関わる「利用者」が参加し、それぞれの役割を担う（内容は表 2.1.2-1 を参照）。これら利用者は、TN に情報を登録したり、情報を閲覧したりする。また、その他の利用者として政府機関のように、閲覧するだけの利用者もいる。

TN エコシステムは、TN に求められる機能を共創によって実現し、TN のシステム基盤である TNP（TN Platform）にシステムの機能、技術や運用支援を提供する企業あるいは公共機関である TNE（TN Enabler）が含まれるが、TN の「利用者」に対するサービスを直接提供する主体であるサービサー（運用主体、あるいは TNSP と呼ぶ）にはならない（TNE はバックヤードとして TNP を実現するための技術及び製品等の提供者の位置づけ）。また、アセッサは、ベンダ、インテグレータの企業としての信用度合い（各種セキュリティ基準への適合・遵守レベル）、ベンダの製品の信用度合いをアセスメントし、結果を TN 上で取引を行う利用者に提供するサービスを行う企業あるいは公共機関であり、エコシステムの一員となる。アセッサは上記の役割から、中立的な組織が担うことを想定している。広い意味では TNE に含まれるが、特殊な役割をもつため、ここでは分離して記載している。

以上のように TN は、各主体がデジタル化された製品信頼情報を流通・取引させる場で、言わばマーケットプレイスを提供するが、TNP を管理・運営する運用主体（TNSP と呼ぶ）は、TN 利用者の利用申請、デジタル ID(DID)の付与、システムの運用管理、利用料の徴収、TNP の各種サービスを利用者への提供などを行う中立的な非営利組織であり、収益協調から独立した関係をとり、エコシステムの外である。

TNSP を中立的な非営利組織とするのは、利益追求を目的とした組織であるとトラストの保証もコスト見合いで限定的となりえるため TN 自体が信用されなくなる可能性があること、また利用者に対する扱いが公平であることが、トラストを扱う基盤としては必須なためである。

図 2.1.1-1 に Trusted Network エコシステムに関わる主体、図 2.1.1-2 に Trusted Network エコシステムと本実証事業の対象を示す。本実証事業では、TN を介して TBOM を安全に流通させる機構・仕組みを対象とする。

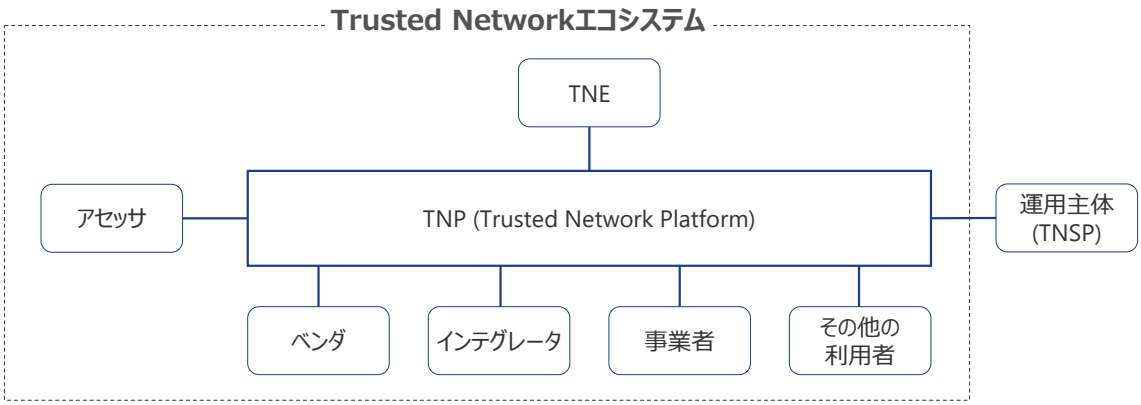


図 2.1.1-1 Trusted Network エコシステム

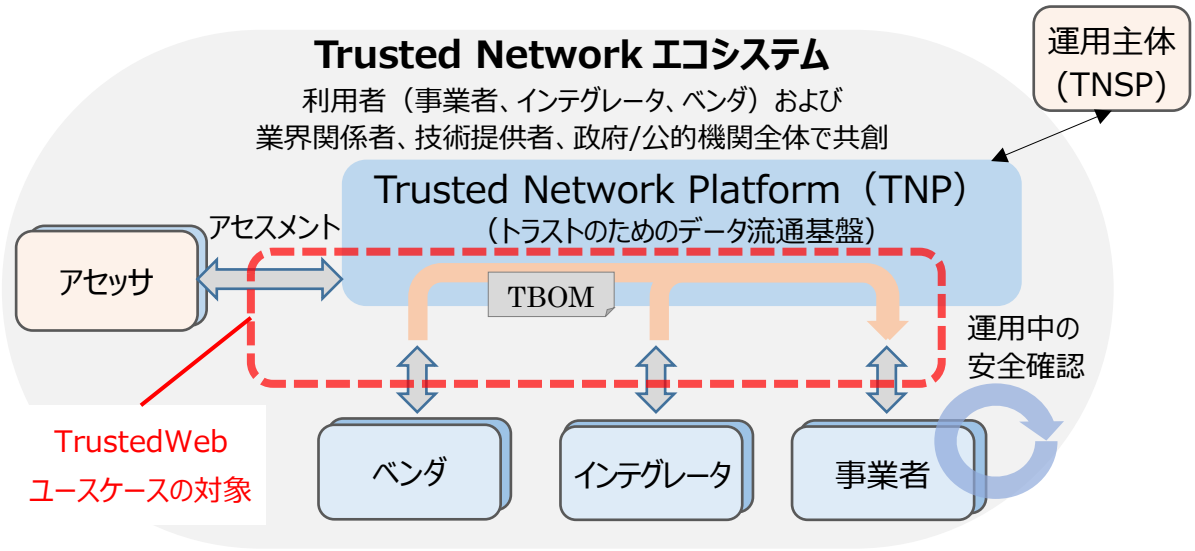


図 2.1.1-2 TN エコシステムと実証事業の対象

2.1.2　実証の範囲

（1）　対象となるユースケース

考案したユースケースと事業スキーム・事業内容を図 2.1.2-1 に示す。主なユースケースについては①～⑪を付番し示した。

本実証事業の対象となる範囲（B 類型で当社が委託を受けた範囲）は、図 2.1.2-1 内に太字（★印）で示したユースケース①～⑥である。

これらの①～⑥のユースケースについては、Trusted Web と基本的に同じ要件を有することから、本実証事業（プロトタイプシステムの企画（要件定義書の作成））を通して Trusted Web との要件レベルでの具体的な整合確認を行うとともに、アーキテクチャ及び実装共通化と相互接続性確保を図った。

ユースケース⑦～⑪は、ユースケース①～⑥の実現によって提供可能となる TN の付加価値である。図 2.1.2-1 に記載されている TN の各機能については 3.1.2 を参照。

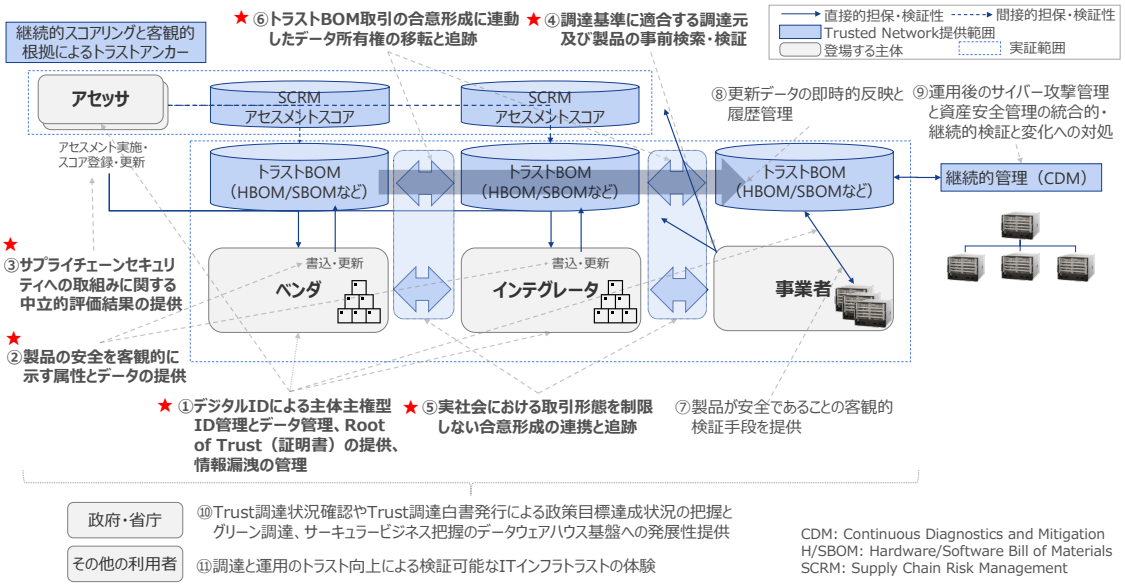


図 2.1.2-1 事業スキーム図

（2） 事業スキームに登場する主体とその概要（事業スキームにおける設定・役割）

各主体には TNP へのユーザ登録によりデジタル ID（DID）が付与され、各主体によるデータのコントロール及び Root of Trust（証明書）の提供、データ提供に関する動的な合意形成とその履歴の管理が可能になるとともに、高度なデータ改ざん防止と永続的な管理を提供する。

表 2.1.2-1 事業スキームに登場する主体とその概要

主体組織	設定・役割	関連 TW ユースケース
アセッサ	現在では、ベンダが提供する製品の生産やインテグレータが提供するシステムのインテグレーションに関し、どのようなセキュリティ基準(*1)にどの程度適合しているのかを横断的かつ共通的に検証するのは困難である。 競争入札時の調達基準に対するコンプライアンスについては、入札者が最終判断を行うため、厳密公平性の下での検証性が担保されているとは言えない状況にある。 アセッサは、自社で提供できるアセスメントメニューを Trusted Network に登録しベンダやインテグレータに提供し、ベンダやインテグレータからの依頼を受けて「アセスメント契約」を締結することで、ベンダの製品、インテグレータが構築するシステムに関する基準適合性の監査と監査結果を提供する役割を担う。このアセスメント契約の態様や有償・無償について Trusted	①、③、⑥

主体組織	設定・役割	関連 TW ユースケース
	Network は一切制約しないが、両者間の合意形成の有無について Trusted Network で確認を行い、合意形成か確認された場合にのみ、アセスメントデータの登録が可能となる。 アセスメントコストと期間を最小化するため、アセスメントの効率化とアセスメント精度を両立させる新規技術を導入し、アセスメントを受ける側の負担を軽減する。 機器を調達するインテグレータやシステムを調達する事業者に対して同一の審査方式に基づいたアセスメント結果の検証性を提供することが可能となるだけでなく、Trusted Network システムが管理するオープンな共通基準によって算定されたレーティング情報も提供する。インテグレータや事業者は、製品間・システム間の比較を行うことで簡易かつ高精度な信頼度の検証が可能となる。 ベンダやインテグレータが既に監査をパスしている基準を有する場合、アセッサが簡易的な確認を実施した上で Trusted Network への登録が可能となる。 アセスメントメニューは基本的に継続的なアセスメントの実施を前提として構成される。自動車の車検や定期健康診断と同様に、アセスメント結果とスコアを担保するためには定期的なアセスメントの実施が必要となるためである。現状の第三者アセスメントサービスはコストと手間の負担が大きいため頻繁にアセスメントを実施することが困難であるが、新規技術の導入によりアセスメント頻度を上げる事が可能となるため、製品やシステムを調達するインテグレータや事業者に対してより正確かつリアルタイムな情報を提供することが可能となり、検証性が向上する。 一方、ベンダやインテグレータが Trusted Network に登録する TBOM についても、そのデータの信頼性（正当なルールやプロセスに基づいて生成され、誤りや偽装が存在しないこと）に対する検証性を提供しなければ、TBOM によって提供される新たな検証性が成立しない。アセッサは、ベンダが提供する製品やインテグレータが提供するシステムの信頼性にお墨付きを与えるだけでなく、彼らが Trusted Network に登録する TBOM の信頼性についておお墨付きを与える事が役割となる。	

主体組織	設定・役割	関連 TW ユースケース
	(*1) 米国 NIST の発行する SP800 シリーズや IEC62443、ISO27001 (ISMS)や関連国際標準、日本の法規及び日本国内でも遵守が必要な他国法規など	
ベンダ	現状では、事業者の基幹インフラを構成する機器（ハードウェア／ソフトウェア）を生産・開発し、インテグレータを介して事業者に提供する供給元である。 Trusted Network では、提供する製品の製品信頼情報（TBOM）提供し、生産する製品に対する製造物責任を有するだけでなく、Trusted Network に提供する製品信頼情報（TBOM）の保守責任も負う。 機器を構成するハードウェアは、ベンダが自社工場で設計・開発・生産する場合や、OEM／ODM ベンダと連携して設計・開発／調達する場合、そして部品サプライヤーから市販品を調達する場合がある。この過程において、相手企業のデューデリジェンス、型式認定や部品認定基準のテスト、部品の受入検査／出荷検査など、様々な取り組みが行われる。 機器に搭載されるソフトウェアを構成する個々の部品やソフトウェアコンポーネントは、ベンダが自社で設計・開発する場合や、部品ベンダ・ソフトウェアベンダに開発を委託する場合、市販品を購入して導入する場合、あるいはオープンソースソフトウェア(OSS)を利用して開発する場合がある。この過程において、委託先のセキュリティに関する取り組み（ガイドライン適合性など）や受入検査／出荷検査など、様々な取り組みが行われる。 このようなハードウェアやソフトウェアの設計や製造、部品調達のプロセスが完全に透明化され、全ての情報が開示されることが理想ではあるが、自社の競争力や有意性原資、知財と知財開発情報、パートナー各社との情報開示契約に関連するため、完全な開示は難しい。また、TBOM の生成方式やフォーマットがバラバラでは、TBOM 自体の共通的な信頼性が担保できなくなり、TBOM の利活用が困難となる。 これらの課題に対応するため、Trusted Network では具体的な TBOM 情報の開示／非開示を TBOM 提供者が主体的にコントロールすることを可能とした。また、TBOM フォーマットや生成手順にデファクトスタンダードを適用することでバラつきを解消し	①、②、④、⑤、⑥

主体組織	設定・役割	関連 TW ユースケース
	た。また、共通的かつオープンなレーティング基準を適用することにより、各社製品・システムのトレーサビリティ範囲や透明性に関する TBOM レーティング情報を提供する。 なお、TBOM に格納するデータの信頼性は、原則としてデータ提供者が担保することとなるが、アセッサによって提供されるアセスメントを受け、アセスメント結果を開示することでデータ信頼性に関する第三者のお墨付きを得る事が可能となる。 Trusted Network を介した TBOM の提供は、TBOM 提供者（ベンダ）と TBOM 受領者（インテグレータまたは事業者）の間の合意形成を経て、TBOM 提供者が提供先を指定することで実行される。 Trusted Network はこの合意形成の態様について有償・無償も含めて一切制約しないが、「トラスト保守サービスの提供」と「トラスト保守サービス契約の締結」を合意形成モデルとして想定する。トラスト保守サービスにより TBOM が提供され、TBOM が提供する価値に見合った合理的な各設定が可能となるため、トラスト価値提供に付帯する新しい経済システムの提供を実現できる。	
インテグレータ	複数のベンダから複数の機器やソフトウェアを調達してシステムを構築し、事業者に提供する。この際、事業者のシステム構成に基づいてベンダから超達した機器やソフトウェア製品の設定を行い、システム全体の保守サポートサービスや運用サービスを提供する。 Trusted Network では、提供するシステムを構成する製品の製品信頼情報（TBOM）更新し、構築したシステムとの合致を担保する形で TBOM 提供し、提供するシステムに対する瑕疵担保責任を有するだけでなく、Trusted Network に提供する製品信頼情報（TBOM）の更新責任も負う。更新内容は TBOM を提供したベンダに通知されるため、ベンダは自社が提供した製品の利用状況や設定状況、特に最新性についての確認を実施することが可能となる。 また、システム設計・設定・テストの過程で実施したテストなどの情報について、TBOM に追加することが可能となる。	①、②、④、⑤、⑥

主体組織	設定・役割	関連 TW ユースケース
	事業者に提供するシステムは、インテグレータ自身が全ての設計・設定・テストを行う場合もあるが、パートナーに一部または全部を委託する場合もある。この過程において、委託先のセキュリティに関する取り組み（ガイドライン適合性など）や受入検査／出荷検査など、様々な取り組みが行われる。 このようなシステムの設計や製造、部品調達のプロセスが完全に透明化され、全ての情報が開示されることが理想ではあるが、自社の競争力や有意性原資、知財と知財開発情報、パートナー各社との情報開示契約に関連するため、完全な開示は難しい。 この課題に対応するため、Trusted Network では具体的な TBOM 情報の開示／非開示を TBOM 提供者が主体的にコントロールすることを可能とした。 なお、TBOM に格納するデータの信頼性は、原則としてデータ提供者が担保することとなるが、アセッサによって提供されるアセスメントを受け、アセスメント結果を開示することでデータ信頼性に関する第三者のお墨付きを得る事が可能となる。 Trusted Network を介した TBOM の提供は、TBOM 提供者（インテグレータ）と TBOM 受領者（事業者）の間の合意形成を経て、TBOM 提供者が提供先を指定することで実行される。 Trusted Network はこの合意形成の態様について有償・無償も含めて一切制約しないが、「トラスト保守サービスの提供」と「トラスト保守サービス契約の締結」を合意形成モデルとして想定する。トラスト保守サービスにより TBOM が提供され、TBOM が提供する価値に見合った合理的な各設定が可能となるため、トラスト価値提供に付帯する新しい経済システムの提供を実現できる。	
事業者	自社の顧客（個人、ユーザ企業、公共機関等）への各種サービスを提供する組織（企業あるいは公共機関、組織）。 事業者のサービス提供に必要となる設備（IT 機器を含む）の導入・構築は、通常、入札を介してシステムインテグレーション	①、②、④、⑤、⑥

主体組織	設定・役割	関連 TW ユースケース
	事業者（インテグレータ）に委託することで行うが、ベンダから直接機器を調達する場合もあり得る。 設備の運用は、事業者自身が行う場合と、インテグレータなど外部に委託する場合がある。 事業者は、継続的なサービス提供の責任を負うため、導入する機器やシステムインテグレーションが問題なく動作し、適正であることをベンダ、インテグレータに求める。 事業者は、Trusted Network に登録されたベンダのトラスト BOM 情報、インテグレータの設定情報を参照し、自社の調達・導入基準、関連法令への適合性を確認する。 調達時の調達要件を定め、Trusted Network を利用することで要件の実効性検証や調達可能な製品やシステムの調達可能性について検証を実施する。調達後は、製品構成の変更監視や真正性検証を継続的に実施するとともに、サイバーセキュリティ攻撃と資産脆弱性管理を統合管理することで IT インフラのトラストの検証と是正を実行する。 事業者は、TBOM 提供者と合意形成することで TBOM の所有権を取得することが可能となるが、同時に更新責任も負う。TBOM を更新することで、現在運用している資産の構成を把握することが可能となり、実資産と TBOM データの突合確認により構成情報と実資産の整合性検証を実施することができる。更新内容は TBOM 提供者（インテグレータ）と資産提供ベンダに通知されるため、インテグレータやベンダは事業者資産の構成やバージョンを常に正確に把握することが可能となり、事業者に対してソフトウェアアップデートを促すことが可能となる（本機能は Trusted Network によって自動で実現される）	
政府・省庁（その他の利用者）	国民生活の安全性を維持・確保するため、重要インフラなどの事業者が調達する IT 機器の安全性の事前審査を書類ベースではなく、TBOM を活用したエビデンス確認のデジタル化による効率的処理を行う。また、導入・運用後の IT 機器の状況（真正性、脆弱性等）を持続的にモニタリングし、状況に応じた政策強化や是正を行い、検証性範囲拡大によりトラストガバナンスを堅持する。	－

主体組織	設定・役割	関連 TW ユースケース
	省庁による利用例としては、が経済安全保障推進法で求められる基幹インフラ事業者の基幹インフラ設備に用いられる IT 機器の事前審査に利用することが考えられる。	
事業者のサービス利用者	利用するサービスが求める SLA（Service Level Agreement：規定サービス品質）等に応じ、事業者が提供するサービスを下支えする IT インフラの客観的なトラストの根拠を検証することが可能となる。 （例：銀行が自社の ATM サービスのシステムに適用されている IT 機器のトラストを、ATM サービスの利用者に提示できるようになる。また、ネットワークサービスプロバイダーが、自社のネットワークのトラストを利用者に提示できるようになる）	–

2.2　社会・経済に与える価値・影響

ネットワーク機器の価値比重がソフトウェアに移行するにつれ、OSS を含むソフトウェアの改ざんや脆弱性のリスクは高まってきている。しかしながら、その対処として要求されるソフトウェア脆弱性対応やリスクスコアリング（危険度合いの見える化）などの付加価値化・収益化は、PC 向けのウイルス対策ソフト（ウイルスパターンファイルを都度更新する付加価値提供によるサブスクリプション・サービス化）のようには進展していない。ハードウェアの OEM（他社ブランド製品を自社ブランド化して導入すること）化が進み、半導体供給や国際情勢が不安定化している昨今、サプライチェーン上での改ざんなどサイバーリスク管理の重要性が日増しに高まってきているが、業界横断で IT 機器の使用部品まで信頼性・安全性に関する情報を提供できる仕組みが存在しないため、サプライチェーン（取引企業）ごとのサイロ化が進行している。

ソフトウェア／ハードウェア改ざんの一律的な自律検知やセキュリティ運用連携の仕組みは確立されておらず、ベンダの規模や資本力に依存した濃淡が回避できない。

サイバーセキュリティ攻撃は PC のソフトウェアからサプライチェーン全体、IT 機器全体に標的が拡大しており、攻撃による社会的影響や経済的被害は拡大の一途を辿っているが、ネットワーク機器を含む IT 機器全体に対して、革新的かつ網羅的なサプライチェーン攻撃対策が遅れている。

事業者やインテグレータが個々に独自対策を講じ始めているが、個別対応による分割損が大きいため経済合理性が低く、ベンダ×インテグレータ×事業者で個別トラフィックが爆発するため現実的な解決策との乖離が大きい。

2.2.1　ユースケースが解決しうる課題

本ユースケースでは以下の課題の解決を図る。事業者が自らの施設・サービスの信頼性を担保しようとしたときの課題として、次のような懸念を解消・解決する必要がある。

(1) 取引先ベンダ、インテグレータ自身の企業としての信頼性に対する懸念
ベンダ、インテグレータ自身が、信頼に足る企業であるかを示すためには、自己申告や評判ではなく、第三者による客観的なアセスメントが必要である。

(2) 機器のハードウェアに対する懸念
従来、ハードウェアの信頼性といえば、部品の MTBF（Mean Time Between Failure 平均故障間隔）から算出するものであったが、ここでは、信頼できるベンダにより、製造されたものであること、製造／設定／運用中を通じて、スパイチップや模造品など不正な部品が混入していないこと、すなわち安全性を確認することが必要。

(3) 機器のソフトウェアに対する懸念
ソフトウェアのセキュリティ上の脆弱性を正しく認識、サプライチェーン上での不正な改ざんがないかを確認するために、搭載されているソフトウェアとして OS やミドルウェア、特にオープンソースソフトウェア、のバージョン等の情報管理が必要である。

(4) 機器がベンダからインテグレータを経て、事業者に納入されるまでの履歴に対する懸念
一般には、機器が製造され、インテグレータにより、システム設定が施され、事業者に納入される。機器のハードウェアとしての所有権が移転される際、正規品として正しくサプライチェーン上で流通されてきたかどうか、その情報（デジタル情報）が改ざんされないように製品取引で付随させることが必要。

(5) デジタル情報と実際に納入されたものの整合性に対する懸念
機器に付随するデジタル情報と実物の機器が整合していることは、必ずしも保証されているわけではない。実物の機器から情報を収集して、デジタル情報と突合する必要がある。

(6) 事業者のガバナンスに対する懸念
インフラ事業者は上記の多岐に渡る懸念を、総合的に、また、継続的に、監督・管理することが期待されるが、必ずしも容易なことではない。

上記の課題を解決するため、TN を考案し、図 2.1.2-1 に示す①～⑥の個別のユースケースに分解して実現を図った。

① デジタル ID による主体主権型 ID 管理とデータ管理、Root of Trust（証明書）の提供、情報漏洩の管理
→ 中央集権型基盤では管理と取引が困難だった製品信頼情報の業界横断かつ統合的な取引が可能となる。

② 製品の安全を客観的に示す属性とデータの管理

→ これまでトラスト（安心できる度合い）は主観的に捉えられてきたが、トラストを上げるための製品信頼情報（TBOM）を管理、その情報充実度をレーティングすることで、客観的にトラストのレベルを捉えられるようにし、個別のデータのやり取りではスケールしなかった製品信頼情報のセキュアな取引が可能となる

③ サプライチェーンセキュリティへの取組みに関する中立的評価結果の管理

→ ベンダの個別製品やインテグレータのサプライチェーンセキュリティに関する取り組み状況の多角的共通的アセスメントと見える化を実現

④ 実社会における取引形態を制限しない合意形成の連携と追跡

→ 既存の調達モデル・プロセスを変えずに新たな価値提供を実現

⑤ TBOM 取引の合意形成に連動したデータ所有権の移転と追跡

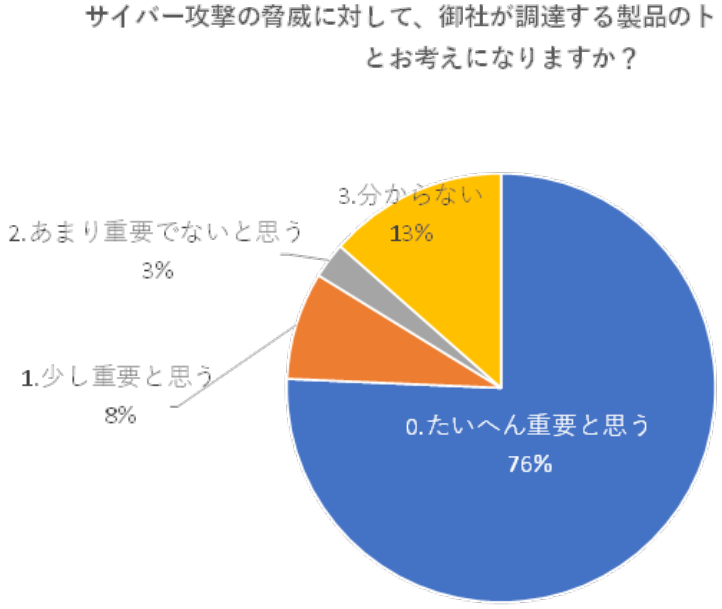
→ ベンダ・インテグレータ・事業者間の個別のやり取りでは管理できない複雑かつ大規模なデータ管理とセキュリティの実現

⑥ 更新データの即時的反映と履歴管理

→ 製品信頼情報の更新と通知にかかるコストの最小化の実現

2.2.2 IT 製品のトラスト向上ニーズ

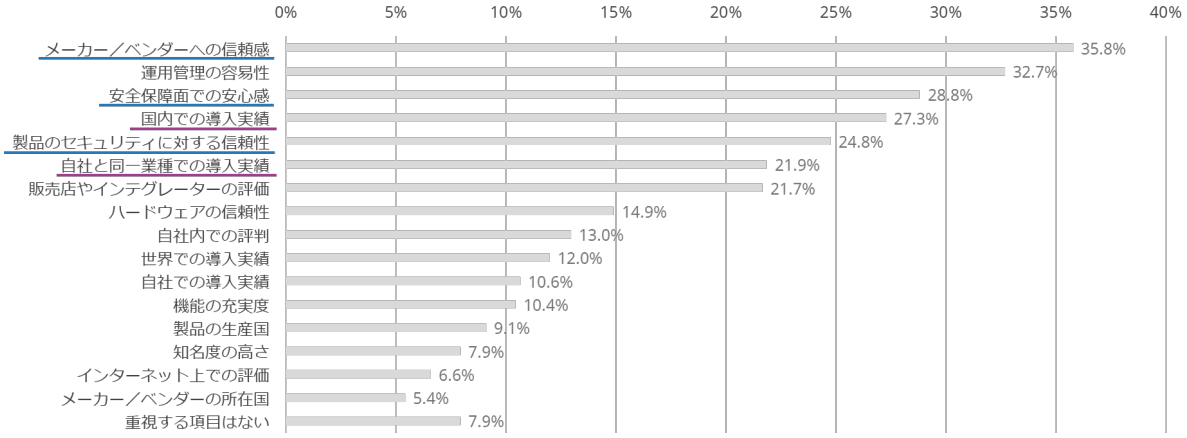
調達する IT 製品の真正性・トラストの向上が必要かどうかについては、日本経済新聞社主催「重要インフラサミット」(2022 年 7 月 26 日)での当社講演「基幹インフラ強靭化課題と解決策 ― エコシステムによる SCM 及びサイバーセキュリティトラストの担保とは？」の聴講者アンケートにおいて、図 2.2.2-1 のとおり重要であるとの認識をもつ割合が高いことがわかった。TN のような仕組みの社会実装に対するニーズがあると考えられる。



2022 年 7 月 26 日, n = 37

図 2.2.2-1 IT 製品のトラスト向上に関するアンケート結果

また、IDC Japan 株式会社が 2021 年に行った企業向け調査において、ネットワーク機器のベンダーやメーカーを選定する際に、価格や必須機能の実装以外で、重視する項目についての結果を図 2.2.2-2 に示す。



Note: 複数回答

Source: IDC's Japan Networking Enterprise Survey, August 2021 (n = 517)

図 2.2.2-2 ネットワーク機器選定において重視する項目

この調査結果から、企業ユーザは機器選定において、ベンダの信頼性、安全保障面での安心感、製品のセキュリティに対する信頼性を重要な判断基準としていることが分かる。

2.2.3 政治・行政、企業活動・経済活動、社会、技術革新における課題の解決

TN で解決し得る課題についてを下記に整理した。

(1) 政治、行政

現在、各省では、IT 資産情報/アラート情報/クラウド情報/認証ログ/ネットワークログ/データ監査ログ等の情報をセキュリティ情報として随時把握している状況であるが、サイバー攻撃の進歩から、政府全体で、「誰が・どこで・いつ・何が起こっているのか」常時把握する必要性が生まれている。これまでのような 1 単体でのセキュリティ状況の把握では、どこからサイバー攻撃が始まり、リアルタイムでどういう影響を受けたのかを把握することが出来ない状況であるが、TN は、リアルタイムでの情報管理の最適化（サプライチェーン上での機器情報及びトレース情報を管理）が可能であるため、常時最新の状況を把握することが可能となる。

(2) 企業活動・経済活動

サイバーセキュリティに関する問題が引き起こす経済的損失に関しては、様々な調査が行われており、6,000 億ドルから 22.5 兆ドルと言われている。日本国内でも 1 社あたり数億円の損失が生じるものと算出されている（出典：総務省（2019）「令和元年版情報通信白書」）。また、サイバーセキュリティが引き起こす 2 次的な損失対応として、ダウンタイム/効率低下/インシデント レスポンス コスト/ブランド毀損・風評被害等が挙げられ、年々サイバー保険料が高騰している。TN の構築により、サイバーセキュリティ対策だけではなく、取り組みを行っている事自体が、企業として優良体アピールとなる可能性が高く、サイバー保険料の最適化に繋がる可能性がある。

（3） 社会

製品の価値は、最終的な成果物として評価されてきたが、製品 1 つ 1 つの部品やインテグレーションにも価値がつき、最終的な製品としての評価が行われようとしている。これは、模造品や開発プロセスでのウイルス混入などの事件から、製造・流通プロセスの過程を評価することで、正しい製品である保証が生まれるからである。よって、製造・流通プロセスの過程を改ざん不可能なデジタル情報資産として、言わば食品に貼付が義務付けられている「ラベル」のように実製品とセットで提供することで、社会の安全性を高め、信用できる製品の流通が可能となる。

（4） 技術革新

様々な業界で IoT の普及が促進されると同時に、1 社だけでの情報ではなく、サプライチェーンの上流企業の CO2 排出量情報を集めてデータの利活用（カーボンニュートラルの Scope3、カーボンフットプリント等）を進めている業界も出てきている。他社を跨ったセキュリティ構築を自社で行うのは、IT エンジニアのコスト・人材不足・マルチベンダ管理の複雑さなどの問題から敬遠されている。また、セキュリティリスクや営業機密に関わる製品情報の提供は、安全性の確保や取引契約の成立した相手に限定することが必要であり、トラストを安全に届けるオープンなプラットフォームはこれまで存在しておらず、実現には TrustedWeb のような新たな技術が必要となる。

●本ユースケース全体として課題解決により提供する価値

図 2.2.3-1 に本ユースケースの具現化により得られる必需的価値（顕在化している課題、ニーズの解決により得られる価値で、満たされないと不満を感じる）と魅力的価値（満たされなくても不満は感じないが、あると満足や感動につながる）を示す。また、それぞれを価値の性質により、機能的価値（機能、性能や品質面において顧客に提供できる価値）、経済的価値（直接的に利益増大やコスト削減を実現できる価値）、情緒的価値（顧客が体感する感覚的・精神的な価値。感動する価値）に分類する。

TN は、機能的、経済的な必需価値とともに、魅力的価値も提供することで、利用者の満足を得ることをめざしている。

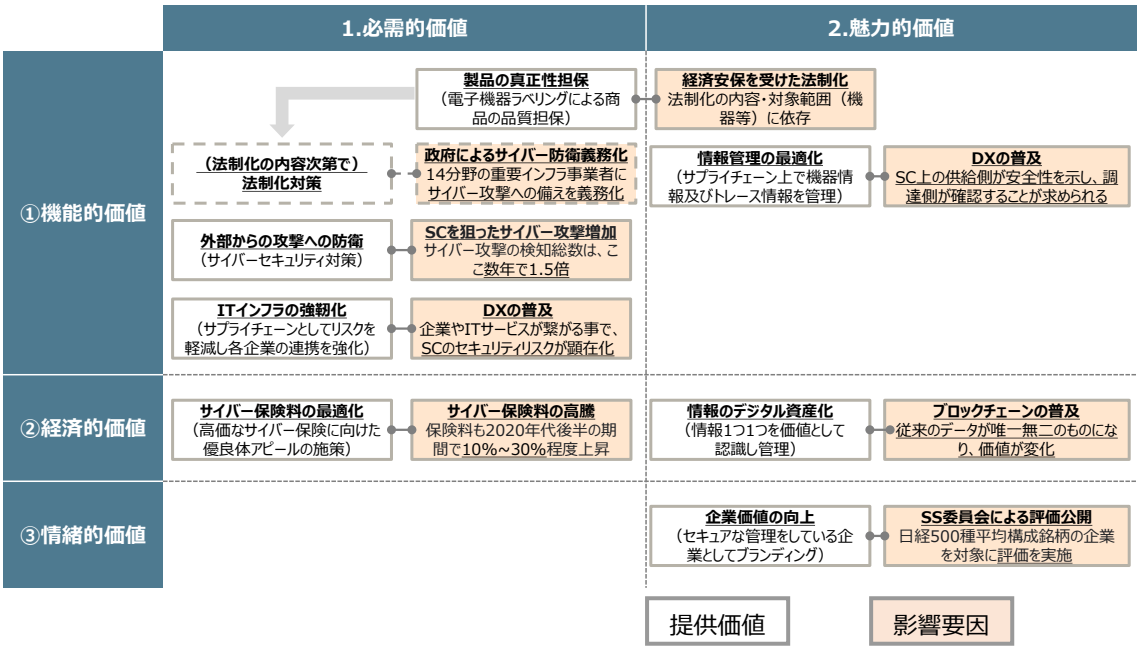


図 2.2.3-1 ユースケースにより提供する価値

2.3 コンソーシアムの体制

本実証事業は、アラクサラネットワークスが委託を受け、アラクサラから一部再委託を行って実施する。以下の体制で推進する。なお、コンソーシアムではないが、アラクサラネットワークスが行う実証は、一般社団法人 沖縄オープンラボラトリにて実施した。

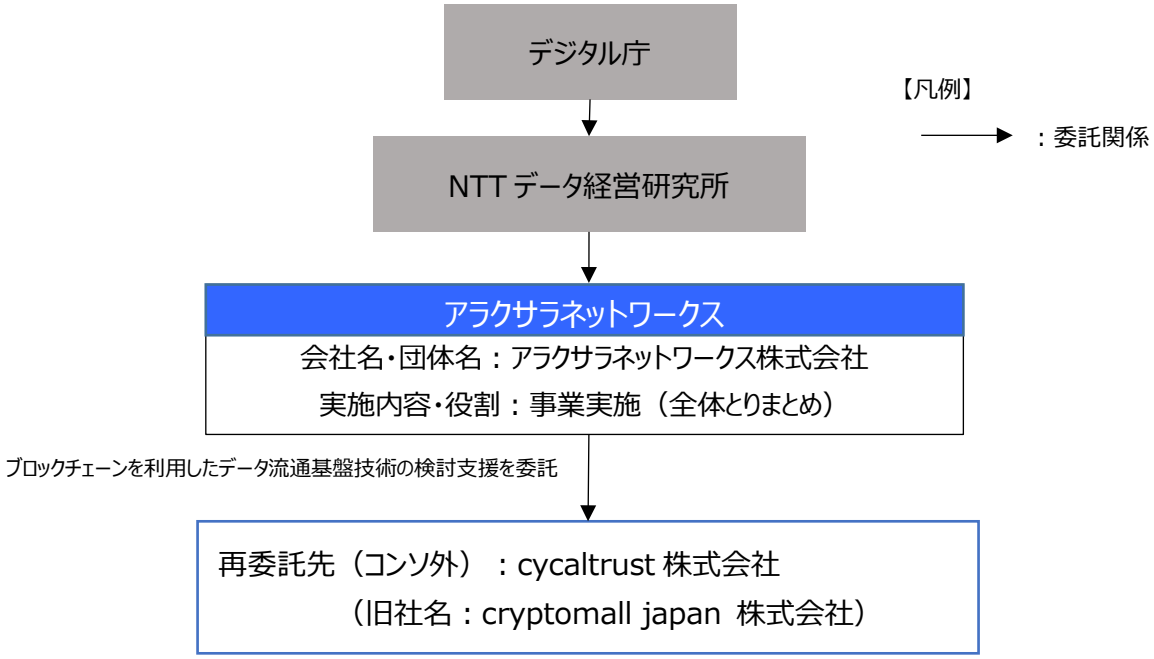


図 2.3-1 コンソーシアムの体制

2.4　実証全体のスケジュール

実証のスケジュールを図 2.4-1 に示す。

市場分析、市場の要件抽出を進めながら、当社が考案済の TN アーキテクチャの見直しと、実装レベルのアーキテクチャ、ユースケースを並行して検討した。また、当社は本実証事業の委託とは別に、自主事業として TN の実装も同時に行った。

実証は、TN のコンセプトやターゲット市場、機能、サービスによる提供価値などを議論するワークショップを９月～１２月、開発したプロトタイプによる実検証を１月～３月にかけて実施した。

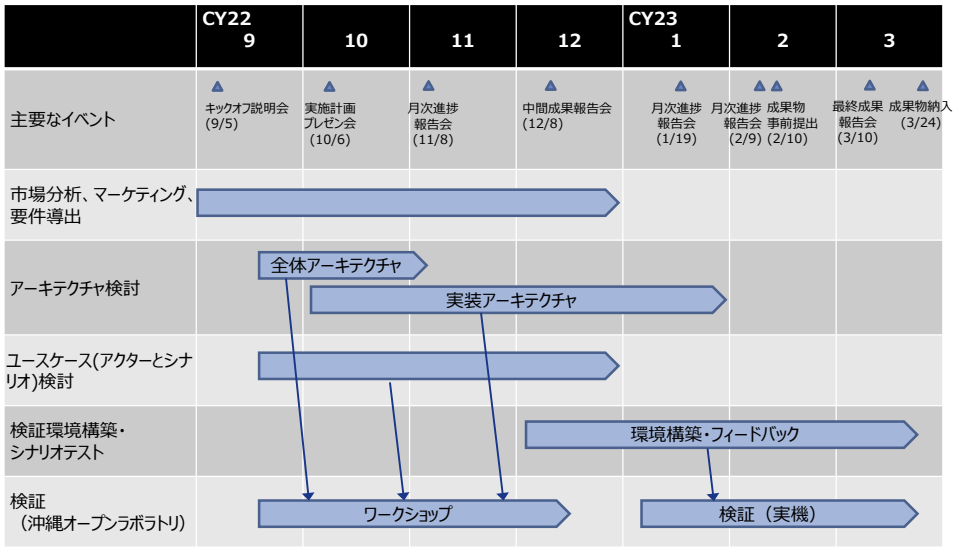


図 2.4-1 実証全体スケジュール

3　実証内容

3.1　実証の実施事項、論点及び判断

3.1.1　Trusted Network プロジェクト

本実証事業（Trusted Web の実現に向けたユースケース実証事業）は、受託したアラクサラネットワークス株式会社（以下、アラクサラ）が、一般社団法人 沖縄オープンラボラトリ（以下、沖縄オープンラボ）の協力を得て発足した Trusted Network プロジェクト（以下、TN-PJ）にて実施した。

TN-PJでは、本実証事業の受託範囲外の実証も含めて実施しており、その部分は自主事業として取り組んだ。TN-PJ では、業界の関係者からの広くご意見をいただき、評価を進めた。

TN-PJ の計画概要を以下に示す。

項目	内容
プロジェクト名	Trusted Network
目的	日本のネットワークインフラのトラストを引き上げる仕組みを構築する
ゴール	ベンダ・インテグレータ・事業者・政府等のその他利用者、複数のステークホルダ目線による Trusted Network の価値体験及び評価検証、課題及び施策提言
プロジェクトの活動内容と期間	● 2022/9/22～12/9　－　ワークショップフェーズ システム・ユースケース及びオンボーディングに関する説明と質疑応答、POV(Proof of Value)手順の展開、POV 環境の構築 ・TN ホワイトペーパーの説明による全体共有と質疑応答 ・各サブシステムのユースケース及びオンボーディングプログラム説明とレビュー ・POV 手順や評価ポイントの合意、課題や施策提言の整理と資料化 ・POV 環境の構築 ● 2022/12/23～3/E　－　検証フェーズ 実システムのハンズオン利用と検証、課題抽出と提言のまとめ、成果発表会を行う また、政府関係者等も招聘し、意見交換（パネルディスカッション）を行う ・TN 導入トレーニング ・TN へのオンボーディングハンズオン ・TN POV ユースケースハンズオン ・利用形態、提供価値、利用容易性の検証と提言の整理 ・実利用に向けた価格、運用形態、サービス提供形態への提言の整理 ● 討論会（パネルディスカッション） ・評価結果発表と関係者によるパネルディスカッション

項目	内容
プロジェクト体制	プロジェクト・オーナー、プロジェクト・マネージャ：アラクサラネットワークス PJ メンバ：沖縄オープンラボ会員、その他一般から募集

（1）TN-PJ ワークショップ内容

#	Topics	月日
1	TN 導入説明、ホワイトペーパーベース概論	2022/9/30(金)
2	全体ユースケース説明、アクター説明、評価ポイント説明	10/7(金)
3	エコシステムプログラム・オンボーディング概論、中間まとめ①	10/14(金)
4	アセスメントとトラストアンカー、基準管理、調達基準改定／調達ユースケース	10/21(金)
5	SCRM、製品信頼情報とは　情報登録方式・手順、調達ユースケース	10/28(金)
6	DID/DAO、合意形成と権利移転・証明書とデータセキュリティ、調達ユースケース 中間まとめ②	11/4(金)
7	真正性管理と真正性確認の仕組み、資産の脆弱性管理、Trust BOM 利活用ユースケース	11/10(木)
8	CDM とオープンサイバーセキュリティ基盤、資産脆弱性・サイバー攻撃・早期警戒システム統合(1)	11/18(金)
9	CDM とオープンサイバーセキュリティ基盤、資産脆弱性・サイバー攻撃・早期警戒システム統合(2)	11/25(金)
10	まとめ、ビジネスモデル協議、検証フェーズ詳細説明	12/2(金)
11	サイバーリスクとサイバー保険	12/9(金)

（2）TN-PJ 実検証内容

#	Topics	月日
1	実検証イントロダクション（POV 環境構成、システム構成、ソフトウェア構成等の説明）、検証準備（アカウント割当方法））	12/23(金)
2	Trusted Assessment システム検証（ベンダ・インテグレータ）のユースケースにおけるデモ・検証 ・アセスメント結果の管理・公開方法の検証、アセスメント技術（TACT[セキュリティ要件分析支援ツール]）詳細説明	2023/1/13(金)
3	Trusted SCRM のベンダ、インテグレータにおけるユースケースのデモ・検証 ・TBOM(製品信頼情報)の情報登録方式・手順の説明、実際に試作したシステムにおいて登録、表示、レーティング等のデモ	1/20(金)
4	Trusted SCRM の事業者（購入製品のエンドユーザ）におけるユースケースのデモ・検証 ・TBOM(製品信頼情報)の検索・参照、調達基準への適合確認などの検証	1/27(金)
5	Trusted SCRM のベンダ、インテグレータ・事業者におけるユースケースのデモ・検証 ・製品の出荷の流れと真正性検証に必要な作業、TBOM のデータ遷移（利用権移転）の流れ	2/3(金)

#	Topics	月日
6	Trusted Asset の事業者における真正性確認ユースケースのシステム検証 ・対象機器が「本物である」かつ「改ざんが無い」ことを TBOM と製品個体情報との突合により確認	2/10(金)
7	Trusted CDM のユースケースのデモ・検証 ・事業者が IT 機器を導入後、運用中に発見あるいは生じた脆弱性や真正性の継続的な確認の流れ	2/17(金)
8	Trusted CDM のユースケースのデモ・検証 ・資産情報作成、脆弱性検知情報 統合、各種センサー情報 統合、CDM を使用した、検知・分析・対処の流れ、サービスインパクトアナリシス、脆弱性スコアリング等の説明・検証	2/24(金)
9	社会貢献ハンズオン ・ビジネスモデル、オファリングメニュー、価格設定等	3/3(金)
10	全体整理・総括	3/10(金)
11	プロジェクト成果発表会・パネルディスカッション	3/17(金)

3.1.2 TN のめざすトラストと基本アーキテクチャ

TN は、高いトラストを提供したいベンダ、インテグレータと、高いトラストを求める事業者のトラスト協働プラットフォーム／マッチングプラットフォームとしてサービス提供する。

ここで言う「トラスト」とは、概念的には、社会的価値及び経済的価値を持続的に創出する信用または信頼関係を示す。具現的には、主体が資産に関連する様々なリスクへの対応に取組み、見える化することで、取引において、他者から見て安心できるレベルの状態であることを示す。様々なリスクとは、地政学的リスク、環境的リスク、経済的リスク、技術的リスク、コンプライアンスリスク、サイバーリスク、評判・風評リスク等を指す。

TN がめざすトラスト充足の要件としては以下があげられる。

- ・トラストを構成する技術や仕組みが透明かつオープンであること
- ・トラストを提供する主体（ベンダ、インテグレータ）がトラストを客観的に証明できること
- ・トラストの提供を受ける主体（事業者）がトラストを客観的に検証できること
- ・中立的な第三者がアセッサとなれること

図 3.1-1 に TN のアーキテクチャを示す。

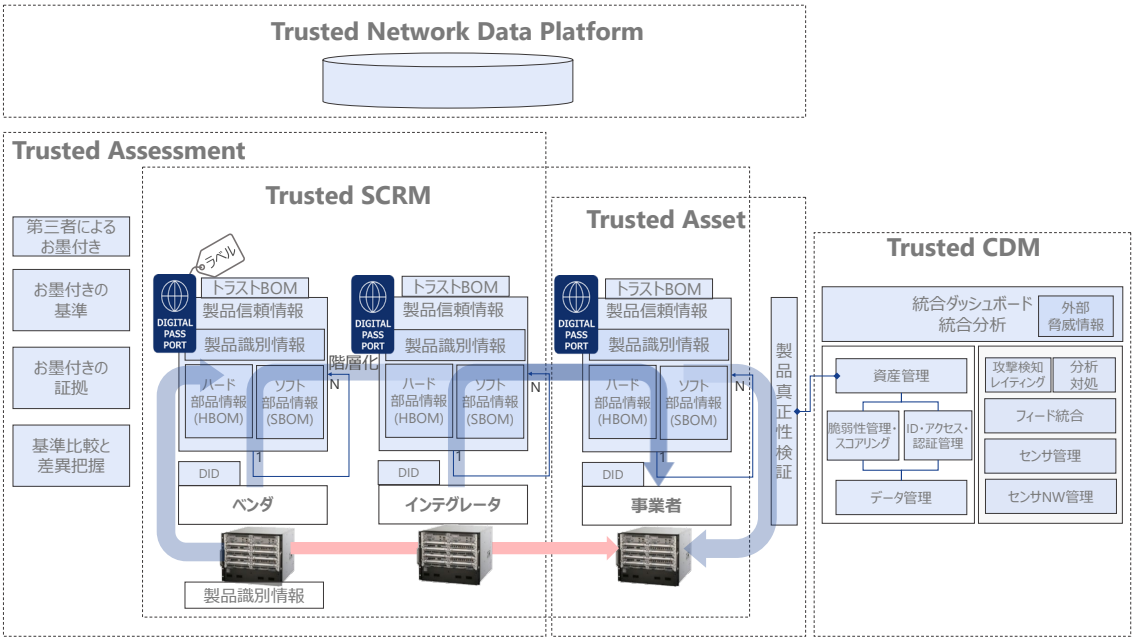


図 3.1-1 TN アーキテクチャ

TN を構成する基本コンポーネントとその主要機能を以下に示す。

TN Data Platform

- ベンダ、インテグレータ、事業者の間で TBOM を安全に登録、変更、開示、所有権の移転等を行うデータ管理基盤
- 高いデータ改ざん防止性と隠蔽性・可用性に加え、国際標準技術を活用した Root of Trust の提供や真正性識別機構を提供するための TN 上で流通・交換されるデータ(TBOM)を格納
- 利用者（ベンダ、インテグレータ、事業者）の識別子（DID）とその属性情報、ベンダ、インテグレータおよび製品のアセスメント結果、製品の TBOM は、データ自体をセキュア・ストレージに格納し、DID や VC の発行、データ（利用者属性情報、アセスメント結果、TBOM 等）の登録・変更の履歴を DID に結び付ける形でブロックチェーンに記録し、改ざんができないようにしている。履歴のみをブロックチェーンに格納するのは、TBOM などのデータ量が膨大であり、ブロックチェーンに書き込むのは性能的に現実的ではないためである。

Trusted Assessment

- ベンダ・製品・インテグレータのサプライチェーンにおけるセキュリティ対策レベルを中立的な第三者（アセッサ）が各種セキュリティ基準への適合度合いをアセスメントし、その結果をレーティングして TNP に登録、開示する機能
- 製品およびそれを扱う主体のそもそもの信用度合いを客観的に評価・査定することで、その後の取引における信頼の起点として保証する

・第三者アセスメント基準と自社調達基準の比較により差異を把握し、事業者の調達基準の妥当性を検証することを可能とする

Trusted SCRM (Supply Chain Risk Management)

・IT 機器のサプライチェーンにおいて、IT 機器のハードウェアやソフトウェアが改ざんされていないかや脆弱性を生じていないかなどを確認する機構を提供する
・事業者の調達・運用に必要となる製品信頼情報（HBOM および SBOM）をデジタル化して格納、充足度（カバレッジ）をレーティングして開示

Trusted Asset

・事業者に納入された IT 機器に対し、製品信頼情報を利活用し、製品真正性検証（ハードウェアとソフトウェア）と最新のトレーサビリティ・構成(設定)情報を取得し、ゼロデイ攻撃対策を含む安全性に対する IT 機器(資産)の対応状況を報告する

Trusted CDM (Continuous Diagnostics and Mitigation)

・米国連邦政府機関で採用されているセキュリティを強化するための継続的な診断と脅威の緩和を行うプログラムである CDM を、政府に限らず一般企業向けに適用可能な仕組みに拡張した継続的攻撃監視と攻撃・脅威緩和のための管理機能
・資産脆弱性やアクセスを管理しデータを含めて保護。資産への攻撃を効率的かつ一元的に管理し、攻撃の危険度と資産の脆弱性を突合管理することで最適な対処の導出を実現

トラスト BOM（TBOM）

・IT インフラ機器を調達する者が必要とする製品信頼情報で、Trusted Network ではトラスト BOM（または TBOM）と呼ぶ。BOM は Bill of Materials の略。
・トラスト BOM にはハードウェアを構成する部品情報(ベンダ名、原産国、型番等)である HBOM、ソフトウェア情報（OSS, 基本ソフトの Ver.番号等）、設定情報、その他からなる SBOM がある。

本実証事業で実証の対象となる TN アーキテクチャの主要コンポーネントを図 3.1-2 に示す。本実証事業では、Trusted Assessment、Trusted SCRM、Trusted Asset とそれらの扱うデータ管理基盤である Trusted Network Data Platform を対象として検証を行う。

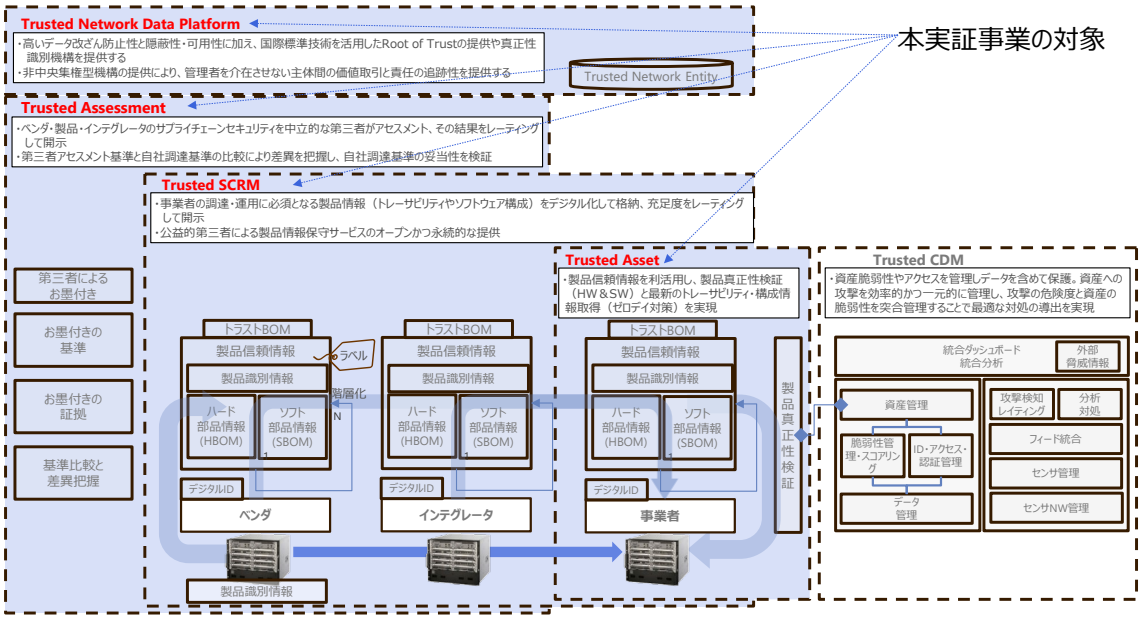


図 3.1-2 TN 基本アーキテクチャと本実証の対象

3.1.3プロトタイプの企画・開発

（１） 要件定義

- 当社と再委託先である cycaltrust 株式会社で TN の機能要件とその実現方式を検討し、必要となる主要件について議論した。論点となったのは以下の事項。
  - ① TN の利用者確認（なりすまし対策）
  - ② TN の登録データ確認
  - ③ ブロックチェーンの選定

- 実現方式はそれぞれ以下のようにした。
  - ① 利用者登録時、TNSP が従来と同様の契約行為を実施し契約を締結することでなりすまし確認を行う。
  - ② TNP によるフォーマットチェックとレーティングを実施。登録者がデータのレーティング結果を確認したうえでデータ登録完了とする。
  - ③ 「Quorum」を使用

- これらの実現方式を選択した根拠・判断理由はそれぞれ以下のとおり。
  - ① 初期登録時に利用者確認をすることで、以後の利用時に DID の認証によりなりすまし出来ない仕組みを確立できるため
  - ② データ登録のためのアクセス管理とデータチェックの仕組みを実現する要件と仕組みを確立する
  - ③ ノード間のネゴシエーション機能（コンセンサス）を備えており、要件を満たすためにもっと

も最適なブロックチェーンを選定

（２） 基本設計

- 当社と再委託先である cycaltrust 株式会社で TN の基本設計のキーポイントについて議論した。論点となったのは以下の事項。
  ① 製品の真正性 確認方法
  ② Dynamic Consent の記録場所
  ③ ベンダ、インテグレータ、その他、事業者への製品の流れ
  ④ TBOM の保存場所
  ⑤ SBOM のフォーマット

- 基本設計の方針はそれぞれ以下のようにした。
  ① 真正性判断の判定基準として、製品識別子（プライマリーキー ）、論理ギャランティーカード （所有者証明）、RFID （実物証明）、ソフトウェアハッシュ（ソフトウェア真正性）の 4 つの認証要素を採用（マルチシグ認証 ）することで認証強度と改ざん防止性を両立
  ② トランザクションはブロックチェーンに記録、属性データはセキュア分散型ストレージ（IPFS）に格納し、相互アクセスのためのハッシュをクロスで保持する
  ③ ブロックチェーンで NFT を移転させ、論理ギャランティーカードの所有者情報を更新することで実現
  ④ ファイル容量が大きくなることから、ブロックチェーン上での処理には時間がかかりすぎるため、セキュア分散型ストレージ（IPFS）に保存する
  ⑤ 国際標準化済、多様な記述様式に対応、市販ツールへの浸透の状況から SPDX を採択。アーキテクチャ的にはその他のフォーマットも適用可能

- これらの基本設計の方針を選択した根拠・判断理由は以下のとおり
  ① 改ざんできない高度な確認方式の確立と運用性の両立
  ② 実用性能を満たしつつ、全ての合意形成の履歴とその属性についてトレーサビリティが提供できるため
  ③ 検証領域の拡大と運用コスト最小化を両立しつつ、現在の調達方式や運用方式にアドオンできるため
  ④ 運用性能を維持しつつ、柔軟かつ高度な検索性を提供できるため
  ⑤ 独自フォーマットとせず、国際標準に準拠するため

（３） システム開発

- 当社と再委託先である cycaltrust 株式会社で TN のシステム開発のキーポイントについて議論した。論点となったのは以下の事項。
  ① TBOM の作成フロー
  ② TBOM の開示請求フロー（個によるデータコントロール）
  ③ TBOM への記録方法と記録内容（検証可能な領域の拡大）

- システムの開発方針はそれぞれ以下のようにした。
  ① ベンダから TBOM を登録してもらい、フロントエンド で TBOM のスコアリング を行った後に、TBOM にスコアリングを紐づける
  ② スマートコントラクトを使ってお互いのウォレット で記録する（データを開示は[1]取引先登録による TBOM レーティング開示、[2]出荷登録による TBOM 内容の開示、の二段階で行う）
  ③ ベンダによって初期登録された際、TBOM 内容と共に初期登録者としてブロックチェーンにトランザクションを記録する。ベンダは最新版がリリースされる都度、TBOM を更新する責任を負う。TBOM の最新情報は過去所有者と現在の所有者に通知され、保守サービスや機器更新判断の契機となる。出荷登録によって TBOM 所有権は出荷先に移動し、TBOM 所有権保有者は TBOM を更新する責任を負う。TBOM 所有者が TBOM を更新することにより、ベンダやインテグレータは製品利用者が現在利用しているバージョンを把握することが可能となる。

- これらのシステムの開発方針を選択した根拠・判断理由は以下のとおり
  ① 標準的な HBOM/SBOM ツールでデータが作成でき、登録時のオペレーション負担を最小化できるため（自動登録など）
  ② 登録者が開示先と開示内容を容易にコントロールできるため
  ③ 更新や更新の取り消しが可能であり、更新が関係者に自動で通知されるため

3.2 検証できる領域を拡大する仕組み

3.2.1 データフロー

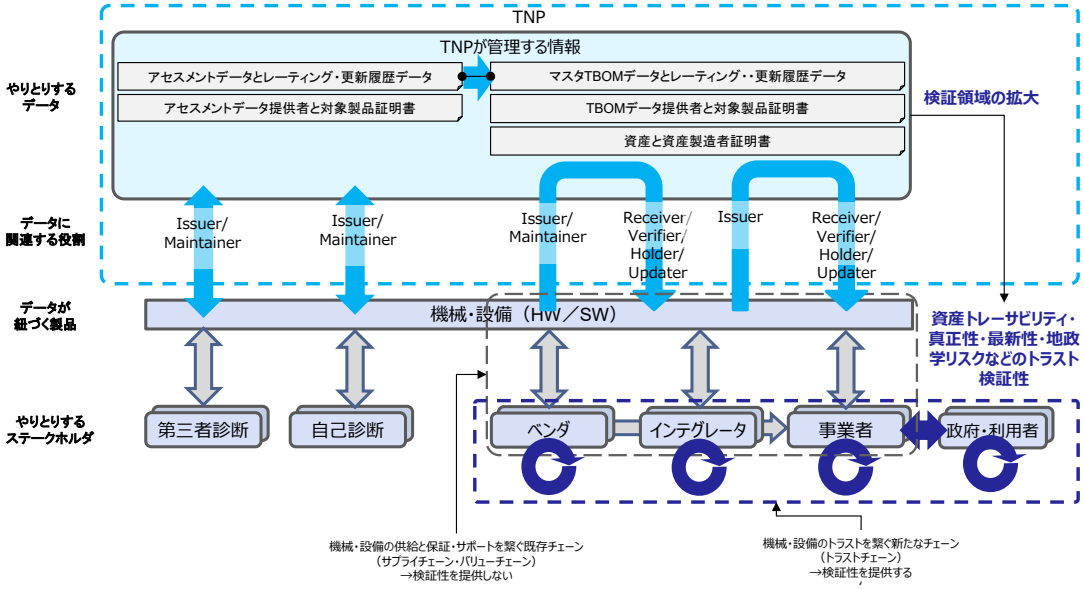


図 3.2-1 各ステークホルダ間におけるデータのやり取りの流れ

各ステークホルダの説明とその間でやり取りするデータは以下のとおり。

•Issuer

- データを生成又は更新し発行する主体

•Maintainer

- Trusted Network では、Issuer のうち初期データの生成発行者が永続的にデータ保守責任を負うため、Maintainer（保守者）というロールを定義している。
- データ保守責任とは、具体的には[1]製品のアセスメント実施者が継続的にアセスメントを実施し、アセスメントデータを更新する責任、[2]製品製造責任者であるベンダが製品のバージョンを管理し、TBOM データを更新する責任、である

•Updater

- Trusted Network では、一部のデータについては Maintainer 以外の Holder が一時的にデータ更新責任を負う。この一時的なデータ更新責任を有する主体を Updater と定義している
- Updater ロールが付帯されるデータについては、「Receiver と Holder／Updater」セクションを参照すること
- Updater によりデータが更新された場合、Maintainer にも更新が通知され、Maintainer は更新情報を確認することができる

•Receiver と Holder／Updater

Trusted Network における Receiver とデータ受信タイミング・データ開示範囲のコントロールは、以下に示す通り三通り提供される。

(1)アセスメントデータのレーティング属性／アセスメント結果属性

- Receiver
  Sender が保有する取引先リストの取引先組織属性に指定された組織（取引先組織属性は二つの組織間で相互認証したタイミングで追加される）
- データ受信タイミング
  データ登録時及び取引先リスト更新時
- 開示範囲コントロール
  レーティング属性は全受信者に開示
  アセスメント結果属性は、各アセスメント結果属性ごとに設定される開示フラグ属性に従って開示
- Holder
  アクセス権を保有する主体
  Sender が保有する取引先リストの取引先組織属性に指定された組織から削除された時点で非 Holder となる
- Updater
  無し

(2)マスタ TBOM データのレーティング属性

- Receiver
  Sender が保有する取引先リストの取引先組織属性に指定された組織（取引先組織属性は二つの組織間で相互認証したタイミングで追加される）
- データ受信タイミング
  データ登録時及び取引先リスト更新時
- 開示範囲コントロール
  全受信者に開示される
- Holder
  アクセス権を保有する主体
  Sender が保有する取引先リストの取引先組織属性に指定された組織から削除された時点で非 Holder となる
- Updater
  無し

(3)個体 TBOM データの HBOM/SBOM/付帯情報属性

- Receiver
  Sender と TBOM データ利用契約を締結した組織（ギャランティーカードの所有者組織属性が契約成立したタイミングで更新される）

- データ受信タイミング
  TBOM データ利用契約成立時（ギャランティーカードの所有者組織属性更新時）
- 開示範囲コントロール
  各 HBOM/SBOM/付帯情報属性ごとに設定される開示フラグ属性に従って開示
- Holder
  アクセス権を保有する主体
  TBOM データ利用契約が解消された時点（ギャランティーカードの所有者組織属性変更時）で Holder から除外される
- Updater
  本データについては Holder ロールに Updater ロールが付帯される
  個体 TBOM データを保有している間、データ更新責任を負う
  個体 TBOM データの更新は、個体 TBOM データの HBOM/SBOM が紐づく資産の構成を変更したタイミングと付帯所法を追加したタイミングとする

•Verifier

- 資産のサプライチェーントレーサビリティ・真正性・最新性・地政学リスクなどのトラスト検証性が提供される主体
- Holder となった時点で検証可能となり、非 Holder となった時点で検証性を失う

図 3.2-2 に TNP が管理する情報とその属性を示す(拡大図を付録 A に示す)。

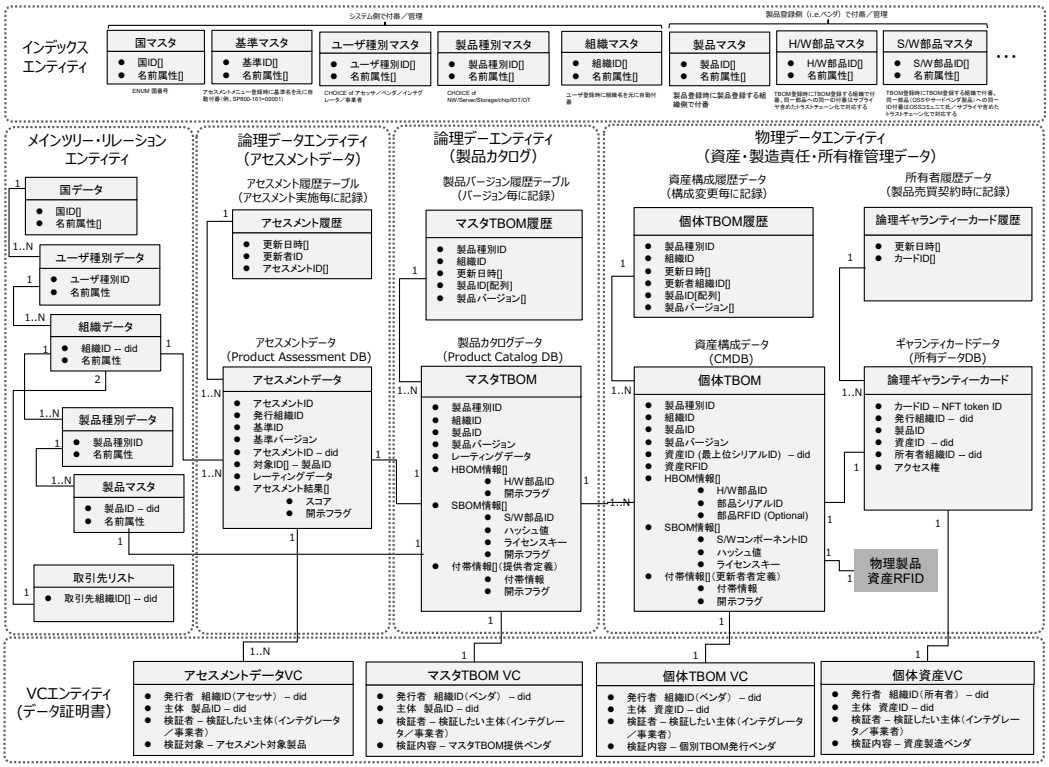


図 3.2-2 TNP が管理する情報とその属性

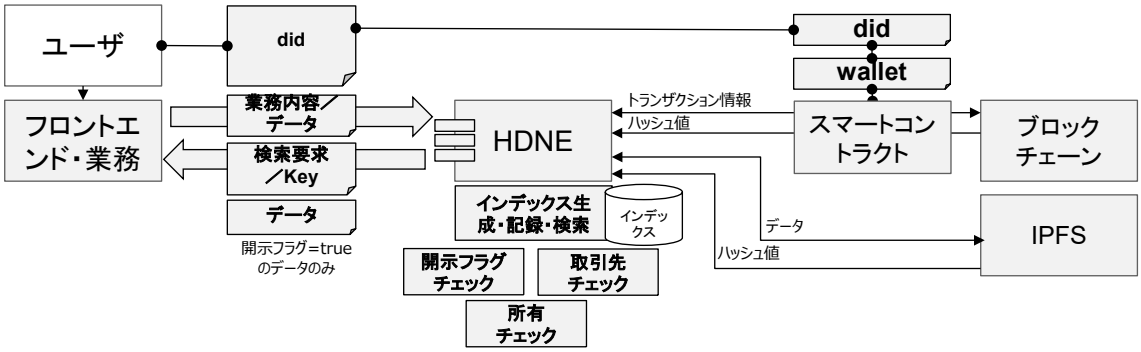


図 3.2-3 TNP が管理する情報とその属性とその保管場所と検索性

図 3.2-3 に TNP が管理する情報とその属性で示したデータの保管場所、検索性を示す。詳細は以下のとおり。

ブロックチェーンを利用した永続的な記録は、その記録の改ざん性を最小化するために有効である。しかし、ブロックチェーンの特性上記録できるデータのサイズと記録性能に制約がある。一方、一般的なデータベースへのデータ格納は、改ざん防止の観点でリスクが高く、Trusted Network で管理するデータの格納方式として適切とは言えない。

上記を踏まえ、TNP が管理するデータの保管はセキュアストレージ（IPFS）によって実現することとし、Trusted Network で管理するデータ格納や更新のきっかけとなったイベントのトランザクション情報のみをブロックチェーンに記録することとする。トランザクション情報とは、その事象が発生したタイムスタンプと事象を起こした組織の ID、そして事象を判別するための情報（Key）とする。
なお、NTP 内部で生成される did や vc の document データも、生成の契機となったイベントがブロックチェーンに、document がセキュアストレージ（IPFS）に記録される。

セキュアストレージ（IPFS）は検索性を提供しないため、セキュアストレージへのデータ格納時にインデックスを生成し、そのインデックスとセキュアストレージ（IPFS）のハッシュ値を組み合わせて一般的なデータベースに記録する機構を提供する。

また、この記録を実行する際、ブロックチェーンに記録されたトランザクションのハッシュ値を組み合わせて記録することで、[1]トランザクションからそのトランザクションで登録・更新されたデータへの検索性、[2]登録・更新されたデータから契機となったトランザクションへの検索性、を提供するとともに、[3]本機構によって記録されたインデックスからトランザクション履歴とデータ更新履歴へのナビゲーションを提供する、Trusted Network では、本機構を Hyper Trusted Data Navigation Engine（HDNE）と呼称する。HDNE のインデックス生成処理は、各データごとに指定されたインデックスキーを抽出して組み合わせることで実施されるため、各データの検索性はデータごとに定義できる事とする。

Trusted Network フロントエンドや業務からのデータアクセスは全て HDNE が提供する API によって proxy されるため、フロントエンドや業務とデータ永続性機構の疎結合化を実現するとともに、相互に置換性を提供することが可能となる。

3.2.2 データフローに登場する主体とその概要

データフローに記載したアセッサ、ベンダ、インテグレータおよび事業者については、表 2.1.2-1 を参照
TN 運用主体は、上記利用者にサービスを直接提供する主体であるサービサーである。2.1.1 を参照
SCRM、Asset、CDM は、TN を構成する基本コンポーネント。3.1.2 を参照

BC 基盤（ブロックチェーン基盤）は、TNE が提供するバックヤード機能の一つ。2.1.1 を参照。

トラストアンカーは、デジタル資産化されたベンダ・製品・インテグレータのアセスメント結果に付帯される、トラストの起点となる証明書／エビデンスを指す。用語集を参照。

想定している主体の属性は、

- アセッサ：情報セキュリティ会社など
- ベンダ：通信機器ベンダ、半導体ベンダなど
- インテグレータ：通信システムインテグレータなど
- 事業者：通信サービスプロバイダー、電力会社など
- TN 運用主体：公益的第三者（独立行政法人、政府機関など）

アラクサラネットワークスは、TNP の技術提供者(TNE)、ならびに、ベンダ（利用者）として TN に参加する。

3.2.3 検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容

（１） TN の利用者確認（なりすまし対策）

・背景

TN は、IT 機器を提供・調達（サプライチェーン）にかかわるさまざまなベンダ、インテグレータおよびデータ利活用者である事業者が参加するトラストデータプラットフォームとしての利用を想定している。

・ペインポイント

Web2.0 ではプラットフォーマーが中央集権的に利用者のなりすましを確認し、利用者の承諾を得ることで様々なデータの利活用を行ってきたが、データがプラットフォーマーに独占的に集約されることに関する様々な課題が認知されてきた。この課題の解決を主目的として、Web3.0 アーキテクチャが広まりつつあるが、プラットフォームが自律的になりすまし対策を実装するのは現在の技術では困難である。同時に、基幹インフラ事業者を始めとする事業者の調達は「契約先企業」に SLA や瑕疵担保責任を求めるため、プラットフォームと契約することは出来ない。

・検証できる領域・課題

まず、Trusted Network の運用を公的的第三者に委ねる事とし、その組織が従来通りの利用者契約や NDA を締結することでなりすましを防止する（＊）。

・検証対象（データ/データのやり取り）、検証方法、検証者、データの保有者、発行者、データ（VC）の置き場所、アクセスコントロールの手法

まず、TNP は、新規利用者に対して、ブロックチェーンのウォレット（秘密鍵、公開鍵、ウォレットアドレスの 3 要素からなる）を生成し、さらにウォレットアドレスを用いて DID を生成し、利用者の登録情報（＊）と DID を紐づけて IPFS にアップロードする。さらに、TNP が利用者の登録情報（属性）に対して VC を発行し、IPFS にアップロードした記録をブロックチェーンに記録する。

上記の登録が済んだ状態で、利用者が TN を利用する際のなりすまし防止として、TNP へのアクセスは DID を用いた認証によって行う。

DID の発行者は TNP が利用者の代行として行う、保有者は利用者で、検証者は TNP となる。検証方法は、DID の検証による。

データの置き場は、IPFS であるが、ブロックチェーンにアップロード記録があるので、改ざんできない。

実際のシステムでは、TNP へのログイン時にパスワード認証し DID・ユーザ ID・パスワードの突合検証を行う。

（＊）TN への利用者の新規利用申請～初期登録時のなりすまし防止は、システムで行うことは現時点では非現実的であり、契約手続き（文書）、契約書と紐づく利用者情報の保管等は手作業が介在する前提としているが、外部電子契約サービスを利用する可能性もある。これを安全に実現することは、事業化において実装上避けて通れない事項である。

（２） TN に登録したデータ（TBOM）の確認

TN に登録した製品信頼情報（TBOM）が正しい提供元（ベンダ、インテグレータ）から登録されているのか、内容の改ざんがないのか（真正性）を検証することが可能。

まず、ベンダは、製品信頼情報（TBOM）を IPFS にアップロードする。アップロード（登録、更新）の履歴とデータへのパスはブロックチェーンに記録する。次に、データ登録の際に得られる識別子を元に DID を生成し、その DID 情報（ベンダの DID、製品の DID、製品情報の IPFS のパス、ベンダの署名）をブロックチェーンに記録する。その上で、ベンダが製品信頼情報の VC を発行する。

・背景

TBOM には、ベンダの機密情報である製品の部品情報が含まれている。
TBOM を改ざんされることなく製品（現物）とともに提供できれば、製品の真正性（改ざんされていないこと）や、脆弱性の有無を確認することができる。

・ペインポイント

多くの事業者が、調達する/所有する IT 機器の TBOM を入手するには、ネットワーク経由で自動的に行えればよいが、改ざんされることなく安全に授受すること、開示先を限定（取引先のみ）にすることは難しかった（膨大な工数が必要）

・検証できる領域・課題

TN に登録されたデータの真正性を確認することが必要

・検証対象（データ/データのやり取り）、検証方法、検証者、データの保有者、発行者、データ（VC）の置き場所、アクセスコントロールの手法

【検証対象】

- 事業者の調達基準に、取引先のベンダ、インテグレータのセキュリティ対応状況が適合しているかどうかアセスメントした結果が正しい登録者によって登録されているか、改ざんされていないか
- ベンダあるいはインテグレータが登録した TBOM が正しい登録者によって登録されているか、改ざんされていないか

【検証方法・検証者・データ保有者・発行者】

利用者が登録されたデータ（TBOM）の真正性を確認するには、VC の署名検証によって行う。VC の発行者はベンダで、保有者は TBOM を更新管理するベンダ、インテグレータ、事業者、検証者はインテグレータ、事業者となる。

【データの置き場所・アクセスコントロールの手法】

TBOM 自体、VC はセキュア・ストレージ（IPFS）に保管するが、保管記録（履歴）と保管場所（パス）は TBOM の DID と紐づけてブロックチェーンに記録してあり、改ざんすることができない。

アクセスコントロールは、DID の認証で行う。ブロックチェーンへの書き込みはウォレットの秘密鍵を使って署名し、署名検証の後に行う。

（３） 製品のアセスメント結果の内容（データ自体）

・背景

TN の利用者であるベンダ、インテグレータの企業としてのセキュリティ対応レベルや、調達候補の製品のセキュリティ対応レベルが、事業者の調達基準に適合するかどうかを判断するためには、一般的に第 3 者によるアセスメントが有効である。

・ペインポイント

企業の IT 機器調達においては、事前にアセスメント結果データを入手する必要がある場合が多いが、回答する側のベンダ、インテグレータがセルフアセスメントに頼ることが多く、実態との乖離の有無は確認できないことが多かった。また基準への対応に時間がかかるため迅速かつ動的に行うことは難しかった。
さらに第 3 者によるアセスメント結果データの提供があっても、それが改ざんされていないことを確実にするには、相手による宣誓などの方法が主流であり、信用は限定的であった。

・検証できる領域・課題

TN によるアセッサのアセスメント結果データの真正性検証

・検証対象（データ/データのやり取り）、検証方法、検証者、データの保有者、発行者、データ（VC）の置き場所、アクセスコントロールの手法

【検証対象】

TN に登録されたアセスメント結果データ

（正しい登録者によって登録されているか、改ざんされていないか）

【検証方法・検証者・データ保有者・発行者】

利用者が登録されたアセスメント結果データの真正性を確認するには、VC の署名検証によって行う。VC の発行者はアセッサで、保有者はアセスメント結果を管理するアセッサ、利用権をもつインテグレータ、事業者、検証者はインテグレータ、事業者となる。

【データの置き場所・アクセスコントロールの手法】

アセスメント結果データ、VC はセキュア・ストレージ（IPFS）に保管するが、保管記録（履歴）と保管場所（パス）は TBOM の DID と紐づけてブロックチェーンに記録してあり、改ざんすることができない。

アクセスコントロールは、DID の認証で行う。ブロックチェーンへの書き込みはウォレットの秘密鍵を使って署名し、署名検証の後に行う。

（４） 製品の真正性確認

・背景

近年のサイバー攻撃は、事業者への攻撃を行うために、事業者の調達する製品にバックドアを仕込むなど脆弱性を生じさせたうえで運用中に攻撃するなどサプライチェーン攻撃の手法が増加している。

・ペインポイント

インテグレータ、事業者は、調達する製品が改ざんされていなかどうか調べる手段をもたない。それも、ハードウェア、ソフトウェアの部品レベルまでとなると、サプライチェーンの上流までさかのぼって、多くのベンダ、インテグレータに問合わせをするなどしかないが、問合せに対応するベンダ、インテグレータも事業者の数、対象製品の数、サプライチェーン上の調査対象企業の数の乗算で、膨大な調査コストを生じる。また、完全な回答が得られるとは限らない。

・検証できる領域・課題

製品（現品）の真正性検証

・検証対象（データ/データのやり取り）、検証方法、検証者、データの保有者、発行者、データ（VC）の置き場所、アクセスコントロールの手法

【検証対象】

製品シリアル番号

開封検知 IC ラベル情報（現品に貼付。剥がすと破壊され読めなくなる RFID を使用）

TBOM

論理 NFT

【検証方法・検証者・データ保有者・発行者】

検証方法は、論理 NFT に記載された製品所有者と真正性確認リクエストを出した主体が一致するかどうかを検証した後、製品（現品）から読みだしたハード/ソフトの構成情報（ソフトウェアはハッシュ値）と TBOM に記載された内容を突合して真正性を検証。また、製品が開封され部品などが不正に交換されていないかどうかは、開封検知 IC ラベルを読み取ることで検証する。

真正性を確認する検証者はインテグレータ、事業者、データ保有者は TBOM を生成・管理するベンダ、インテグレータと製品を調達した事業者、TBOM、VC、論理 NFT はベンダ、インテグレータにより発行・更新される。

【データの置き場所・アクセスコントロールの手法】

真正性検証用のデータ TBOM、論理 NFT は TNP に格納され、製品シリアル番号と開封検知 IC ラベルは製品からコマンド/API で読みだす、あるいは貼付されている。

TBOM、論理 NFT、VC はセキュア・ストレージ（IPFS）に保管するが、保管記録（履歴）と保管場所（パス）は TBOM の DID と紐づけてブロックチェーンに記録してあり、改ざんすることができない。

3.2.4 本システムで形成を目指す合意とその履行のトレースの内容

下表に本システム上で管理する合意形成とその履行のトレースに関する説明を整理した。

合意形成やトレースのデータ構造やデータ保管方式、更新履歴の管理方式、トレースの為の検索性提供手法については、3.2.1 データフローを参照すること。

表 3.2-1 合意とその履行のトレースの内容

合意の主体	合意の対象 （データ::属性）	合意の条件 合意取り消しの条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
製品を提供するベンダと製品を調達するインテグレータ（又は事業者）	取引関係（取引先リスト::取引先組織[]）	ベンダーインテグレータ間で取引先登録申請と承認のシーケンスが成立すること ベンダーインテグレータ間で取引解消申請と承認のシーケンスが成立すること	取引先データと取引先リスト更新履歴（Trusted Network の外では NDA を含む契約書のサインが行われる）	取引先を管理するベンダとインテグレータ	ベンダとインテグレータは取引先確認画面で現状の取引先を、取引先追加・解消画面で取引先の追加と削除を、取引先履歴画面で過去の登録・解消履歴をトレースすることができる。	可能。合意取り消しの条件が成立し、取引先リストから取引先を削除することで可能
システムを提供するインテグレータとシステムを調達する事業者	取引関係（取引先リスト::取引先組織[]）	インテグレーター事業者間で取引先登録申請と承認のシーケンスが成立すること インテグレーター事業者間で取引解消申請と承認のシーケンスが成立すること	取引先データと取引先リスト更新履歴（Trusted Network の外では NDA を含む契約書のサインが行われる）	取引先を管理するインテグレータと事業者	インテグレータと事業者は取引先確認画面で現状の取引先を、取引先追加・解消画面で取引先の追加と削除を、取引先履歴画面で過去の登録・解消履歴をトレースすることができる。	可能。合意取り消しの条件が成立し、取引先リストから取引先を削除することで可能
製品を提供するベンダと製品を調達するインテグレータ（又は事業者）	TBOM 所有権（論理ギャランティーカード::所有者組織 ID）	ベンダーインテグレータ（事業者）が取引先であること。 トラスト保守契約等によりベンダーインテグレータ間で TBOM 所有権移転に関する合意が形成され、その合意形成結果がベンダによって Trusted Network に入力され、合意相手が承認すること。 インテグレーター事業者間で TBOM 利用取引解消申請と承認のシーケンスが成立すること	論理ギャランティーカードデータと利用者組織 ID の更新履歴（Trusted Network の外では NDA を含むトラスト保守サービス（例）の契約が締結される）	TBOM 所有権について合意形成した二社	ベンダは自社保有 TBOM 一覧から保有する TBOM を管理できる。ベンダは出荷機能により TBOM の所有組織を合意形成したインテグレータ（又は事業者）に変更する事ができる。所有組織変更時には、所有権変更先組織との間で確認が行われる。	可能。出荷の取り消しにより論理ギャランティーカードの所有組織 ID を更新することで可能。
システムを提供するインテグレータとシステムを調達する事業者	TBOM 所有権（論理ギャランティーカード::所有者組織 ID）	インテグレーター事業者が取引先であること。 トラスト保守契約等によりインテグレーター事業者間で TBOM 所有権移転に関する合意が形成され、その合意形成結果がインテグレータによって Trusted Network に入力され、合意相手が承認すること。 インテグレーター事業者間で TBOM 利用取引解消申請と承認のシーケンスが成立すること	論理ギャランティーカードデータと利用者組織 ID の更新履歴（Trusted Network の外では NDA を含むトラスト保守サービス（例）の契約が締結される）	TBOM 所有権について合意形成した二社	インテグレータは自社保有 TBOM 一覧から保有する TBOM を管理できる。インテグレータは出荷機能により TBOM の所有組織を合意形成した事業者に変更する事ができる。所有組織変更時には、所有権変更先組織との間で確認が行われる。	可能。出荷の取り消しにより論理ギャランティーカードの所有組織 ID を更新することで可能。
アセッサとアセッシ	アセスメント依頼（アセスメントデータ）	アセッシがアセッサとアセスメントメニューを選択しアセスメントを依頼し、アセッサが合意する	アセスメントの実施（Trusted Network の外ではアセスメント契約書のサインが行われる）	アセッサとアセッシ	アセッシは Trusted Network でアセスメント依頼を行い、アセッサとの間でアセスメン	可能。アセスメントデータを無効化し、履歴に追加すうることで可能。

合意の主体	合意の対象 （データ::属性）	合意の条件 合意取り消しの条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
		アセッシ又はアセッサがアセスメントのキャンセルを選択し、相互にキャンセルに合意する			ト契約を締結し、そのあとアセッサがアセスメントを承諾する。	
アセッサとアセッシ	アセスメントレーティング（アセスメントデータ::アセスメント結果とレーティングデータ）	アセッシが結果とレーティングを確認し、承諾すること。 アセッシが結果とレーティングの承諾を取り消すこと。	アセスメント結果とレーティング	アセッサとアセッシ	アセッシは Trusted Network でアセスメント結果とレーティングの確認を行い、承承諾や承諾のキャンセルが可能	可能。 アセスメント結果とレーティングの承諾を取り消すことで可能。
ベンダ と TNP	TBOM レーティング結果	ベンダが TBOM を登録し、レーティング結果に合意すること ベンダが TBOM の開示を停止し、再度 TBOM を更新する	TBOM レーティング	ベンダ TNP	ベンダは TBOM 登録画面 TBOM を登録し、レーティング確認画面で結果を確認、承認か TBOM の登録のキャンセルを選択できる	可能。 TBOM 登録のキャンセル又は再登録

3.3　6 構成要素との対応

3.3.1　検証可能なデータ

（1）　検証対象

① ユーザ情報の内容（署名したアイデンティティ）

② 製品および TBOM 情報の内容確認（データ自体）

③ 製品のアセスメント結果の内容（データ自体）

④ 製品シリアル番号、開封検知 IC ラベル情報、TBOM 情報と論理 NFT（署名したアイデンティティ、データ自体、製品そのもの）※

※論理 NFT は、TN 上で IT 機器に対する契約や所有状況を表す NFT。契約締結によって所有者が変わり、所有者の履歴情報が管理される。NFT（Non-Fungible Token）については用語集を参照。

（2）　検証者

① ベンダ、インテグレータ、事業者

② インテグレータ、事業者

③ ベンダ、インテグレータ、事業者

④ インテグレータ、事業者

3.3.2　アイデンティティ

（1）　アイデンティティとして想定されるもの

IT 機器メーカー、半導体メーカー、ソフトウェアベンダ、IT 機器のシステムインテグレータ、基幹インフラ（重要インフラ）事業者[通信事業者、電力会社、銀行など]、アセッサ[情報セキュリティ監査サービス会社など]

（2）　アイデンティティ管理システム

DID とそれに紐づけられた属性情報を記録したブロックチェーン

（3）　アイデンティティグラフとして想定されるものは何か

サプライチェーンにおいて、ベンダ間、ベンダ - インテグレータ間、インテグレータ間、インテグレータ-事業者間、 ベンダー-事業者間、事業者間で可視性（TBOM の閲覧可能範囲）の違いが存在する。

また、ベンダ、インテグレータ、事業者の間で、取引前と取引後で、可視範囲（TBOM の閲覧可能範囲）が変わる

これらの可視性を実現するするため、アイデンティフラグで識別を可能とするとともに、取引状態のステートフル管理を必要とする。

3.3.3 ノード

（1） Wallet の使用有無

TNP からブロックチェーンにアクセスするノード(エンティティ。具体的にはベンダ、インテグレータ、事業者)に対して、Wallet を生成する。それぞれのエンティティを識別するための DID は Wallet アドレスを利用して生成する。

TN で採用しているブロックチェーンは Quorum であり、Quorum の仕様に基づく Wallet を実装している。

Holder であるベンダ、インテグレータ、事業者においては Quorum の Wallet ベースで実装しており、申請先（Verifier）のインテグレータ、事業者、証明書発行団体（Issuer）であるベンダ、インテグレータおよびアセッサにおいてはプロトタイプを開発した。

（2） 合意形成がされているか、されている場合その手段

Dynamic Consent として Quorum のスマートコントラクト機能を利用

TN において Dynamic Consent は、

・IT 機器の調達、トラスト保守サービスの契約などの合意（承認/非承認の履歴）

・データの開示可否、開示範囲（開示先）、開示条件などの合意

に用いる。

Dynamic Consent は、データ取得リクエストに対して各 API からブロックチェーンに問い合わせてチェックすることで実現している。

（3） データのやり取りの記録場所

ブロックチェーン（Quorum）

3.3.4 メッセージ

（1） コネクションオリエンテッドかメッセージオリエンテッドか

・TN の利用者（ベンダ、インテグレータ、事業者）の識別子（DID）に対する VC を発行[リクエスト+レスポンス]

・製品情報(製品名などの基本情報)の VC を発行[リクエスト+レスポンス]

・ベンダ、インテグレータおよび製品に対するアセスメント結果の VC を発行[リクエスト+レスポンス]

・ベンダの製品の TBOM に VC を発行[リクエスト+レスポンス]

・TN 利用者（ベンダ、インテグレータ、事業者）による利用者の属性情報の取得[リクエスト+レスポンス]

・TN 利用者（ベンダ、インテグレータ、事業者）による利用者のアセスメント結果の取得[リクエスト+レスポンス]

・製品および TBOM の閲覧[リクエスト+レスポンス]

・製品および TBOM の所有権の移転[リクエスト+レスポンス]

3.3.5 トランザクション

（1） データのやり取りの記録・検証はできるか

・全ての[リクエスト＋レスポンス]はトランザクションとしてブロックチェーンに記録し、検証が可能

3.3.6 トランスポート

（1） トランスポートのプロトコル

・TN 上では Quorum のノード間通信機能

3.4　本実証で企画・開発したシステムの概要

3.4.1　動作シーケンス

以下に主体ごとに TN へのオンボーディング（参加）、Trusted Assessment、Trusted SCRM のそれぞれについて、動作シーケンスを示す。

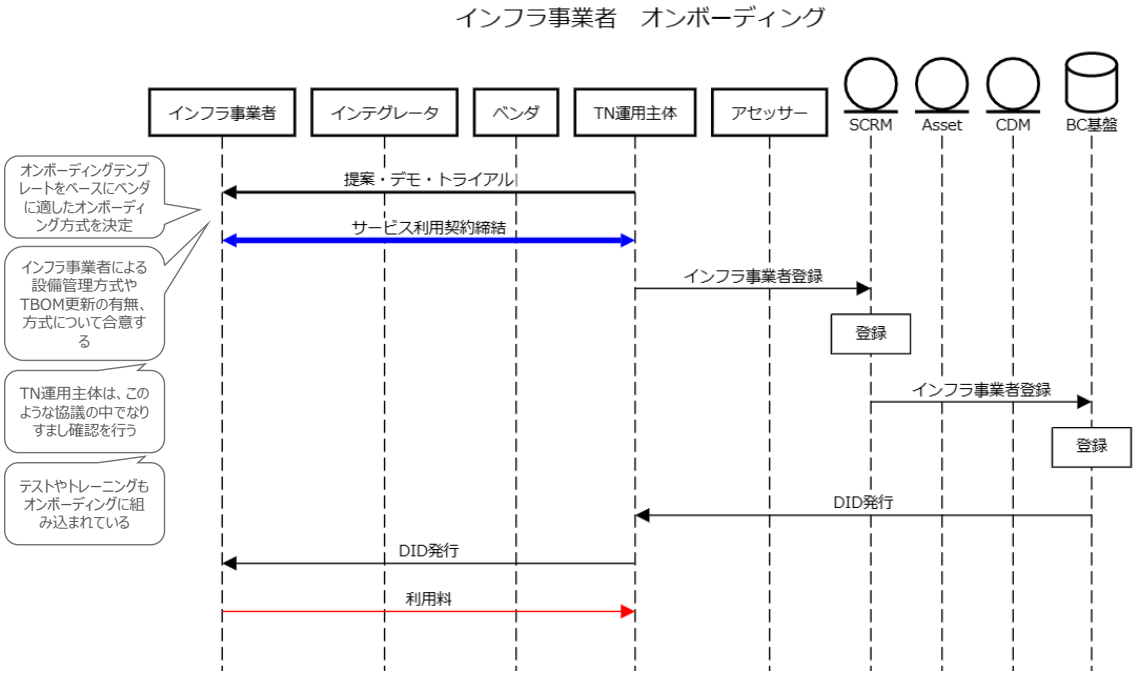


図 3.4-1 事業者　オンボーディング

(注) 図では事業者として「インフラ事業者」（社会インフラを提供する事業者）の例を記載

・事業者が TN の利用契約を行った後、TN のサプライチェーン上で取引を行うために Trusted SCRM に利用者登録をする
・事業者の識別子は、ブロックチェーン（BC 基盤）に当該事業者用のウォレットのウォレットアドレスを DID に設定して生成する。事業者は、運用主体（TN の利用者登録を行う）に DID の発行を依頼し、運用主体は利用者による DID 発行を代行する。
・事業者利用者の登録情報は、DID 識別子に紐付けてセキュア・ストレージ（本実証では IPFS を使用）にアップロードし、TNSP が利用者の VC 発行、アップロードした記録をブロックチェーンに記録する（シーケンス図ではセキュア・ストレージの記載を省略）

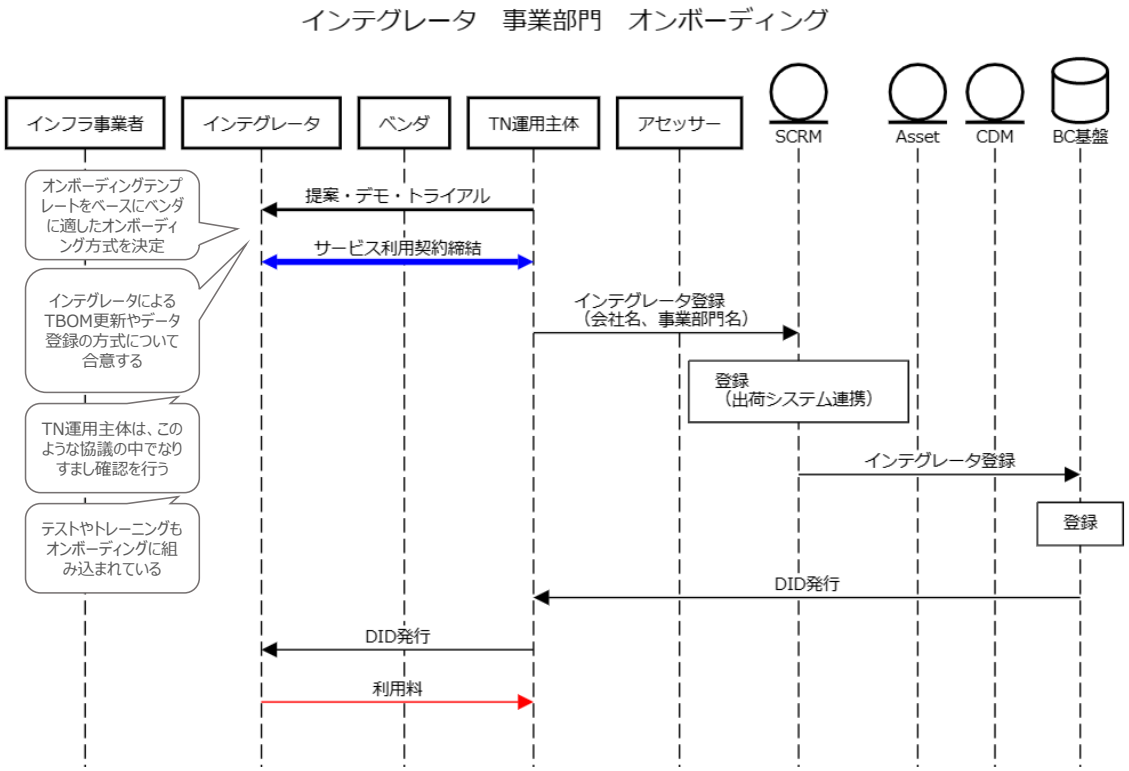


図 3.4-2 インテグレータ　オンボーディング

(注) 図ではインテグレータの事業部門が TN にオンボーディング（利用登録）する例を記載

・インテグレータが TN の利用契約を行った後、TN のサプライチェーン上で取引を行うために Trusted SCRM に利用者登録をする。大手インテグレータは、ベンダとしての事業も併せ持つケースがあることから、インテグレーションを行う事業部門単位での登録を想定している。そうしないと、競合ベンダの情報をインテグレータのふりをして閲覧することが可能となってしまうため。

・インテグレータの識別子は、ブロックチェーン（BC 基盤）に当該事業者用のウォレットのウォレットアドレスを DID に設定して生成する。TN の利用者は、運用主体（TN の利用者登録を行う）に DID の発行を依頼し、運用主体は利用者による DID 発行を代行する。

・インテグレータの登録情報は、DID 識別子に紐付けてセキュア・ストレージ（本実証では IPFS を使用）にアップロードし、TNSP が利用者の VC 発行、アップロードした記録をブロックチェーンに記録する（シーケンス図ではセキュア・ストレージの記載を省略）

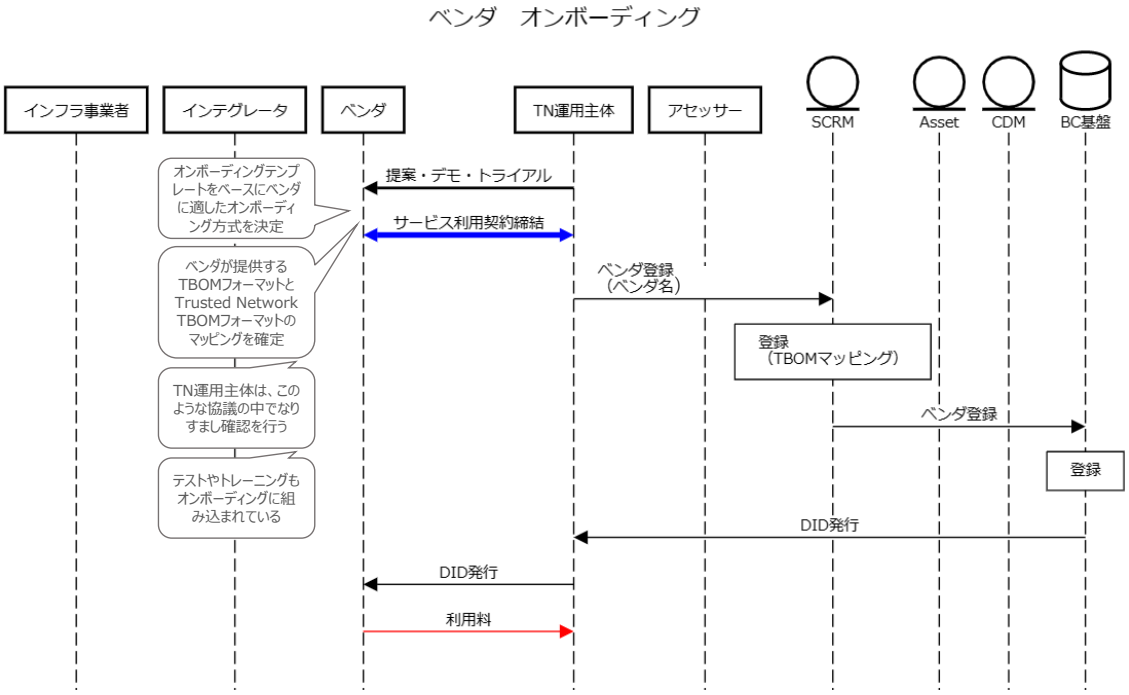


図 3.4-3 ベンダ　オンボーディング

・ベンダが TN の利用契約を行った後、TN のサプライチェーン上で取引を行うために Trusted SCRM に利用者登録をする。その際、TN で使用する TBOM のフォーマットとベンダが提供する TBOM のフォーマットの関係も登録しておく。TBOM のフォーマットには、いくつかの規準、バージョンがあり、異なるフォーマット間で項目の対応関係を定義（マッピング）し、処理ができるようにするためである。

・ベンダの識別子は、ブロックチェーン（BC 基盤）に当該事業者用のウォレットのウォレットアドレスを DID に設定して生成する。TN の利用者は、運用主体（TN の利用者登録を行う）に DID の発行を依頼し、運用主体は利用者による DID 発行を代行する。

・ベンダの登録情報は、DID 識別子に紐付けてセキュア・ストレージ（本実証では IPFS を使用）にアップロードし、TNSP が利用者の VC 発行、アップロードした記録をブロックチェーンに記録する
（シーケンス図ではセキュア・ストレージの記載を省略）

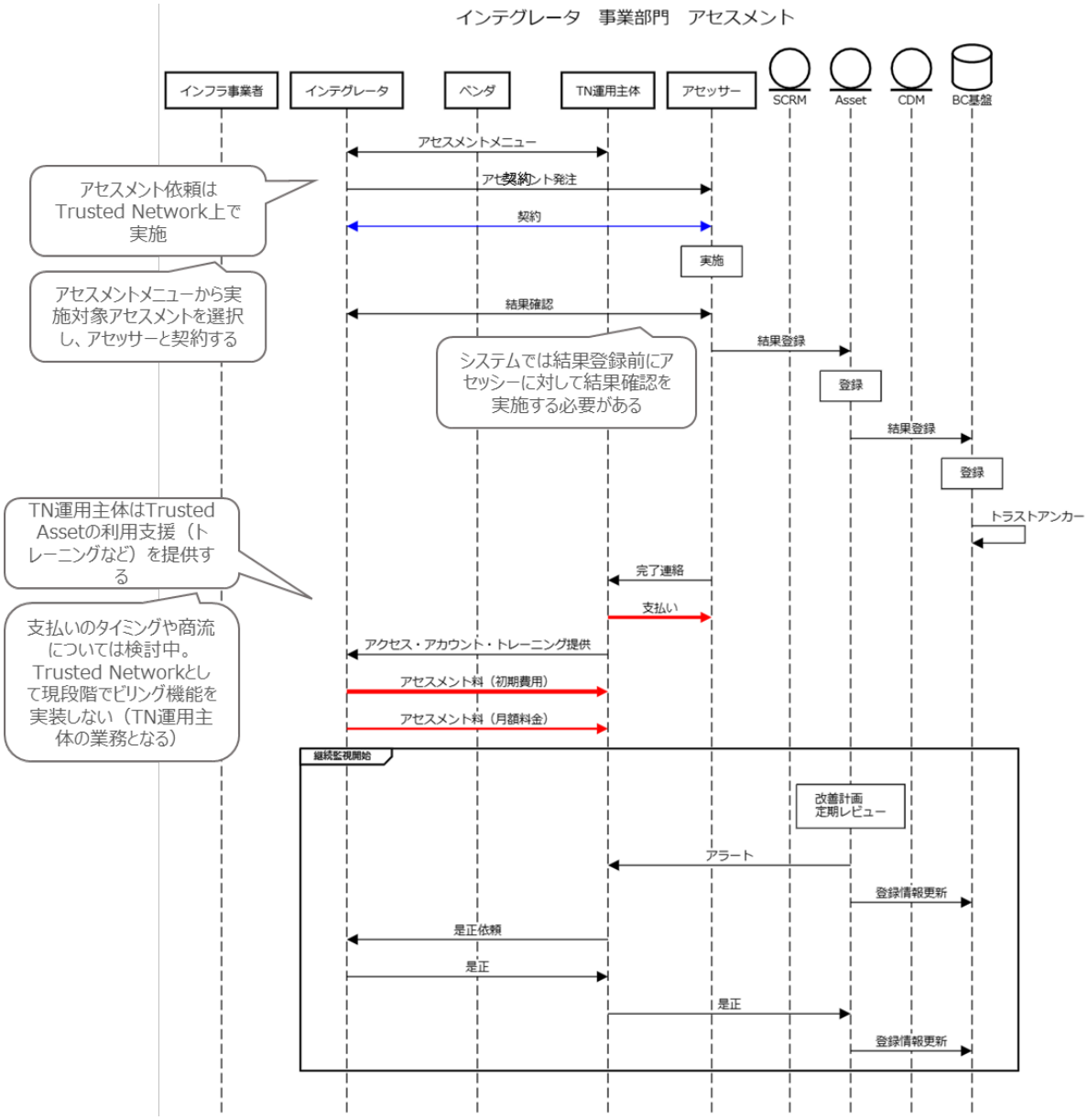


図 3.4-4 インテグレータ　事業部門　アセスメント

・インテグレータのアセスメント結果を TNDP に登録したことをブロックチェーン（BC 基盤）に記録する。

・アセスメント結果を登録した上で、トラストの起点となる証明書（エビデンス）を TN 上で発行する（この証明書のことをトラストアンカーと呼ぶ）。

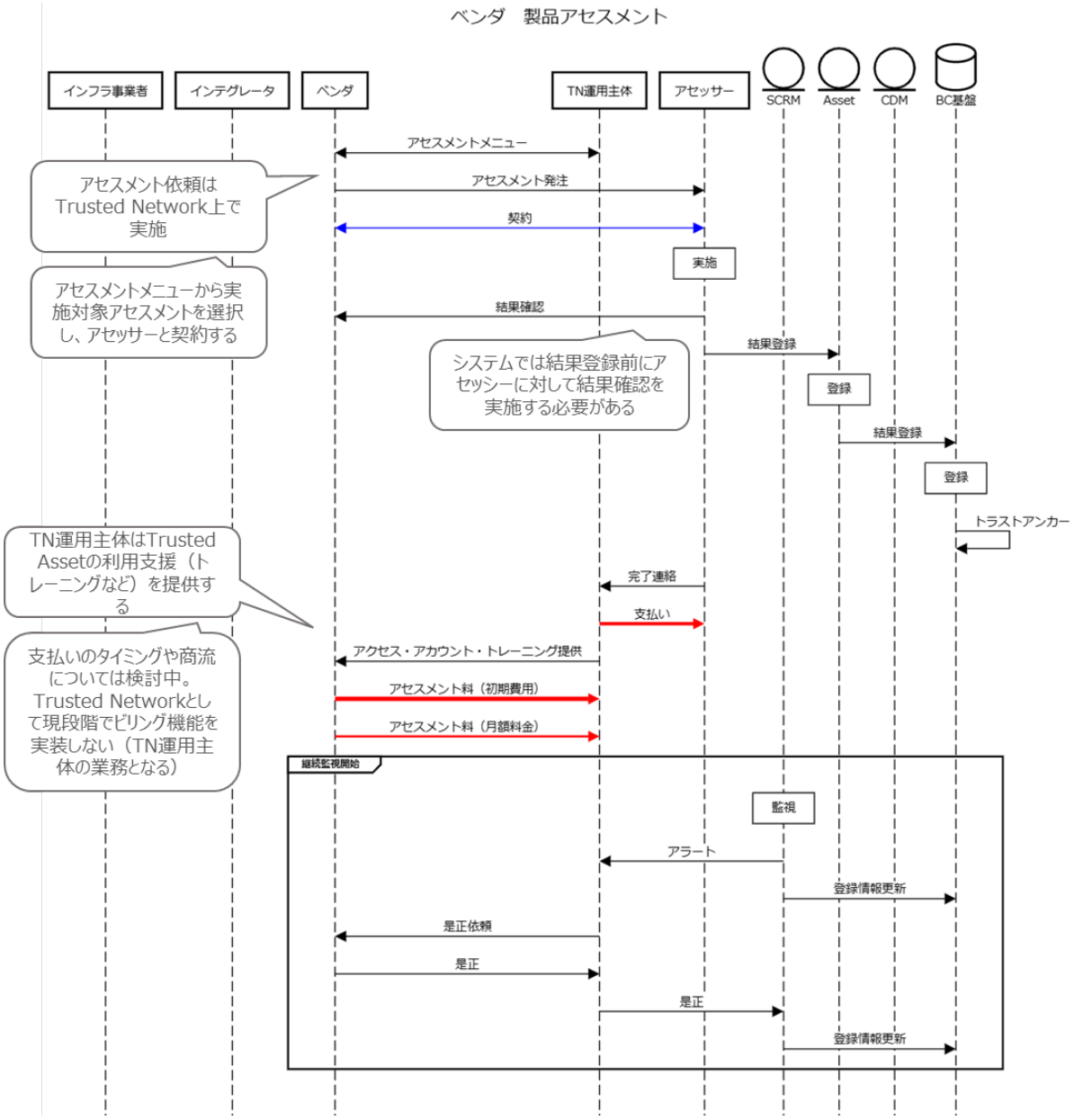


図 3.4-5 ベンダ 製品 アセスメント

・ベンダおよび製品のアセスメント結果を TNDP に登録したことをブロックチェーン（BC 基盤）に記録する。

・アセスメント結果を登録した上で、トラストの起点となる証明書（エビデンス）を TN 上で発行する（この証明書のことをトラストアンカーと呼ぶ）。

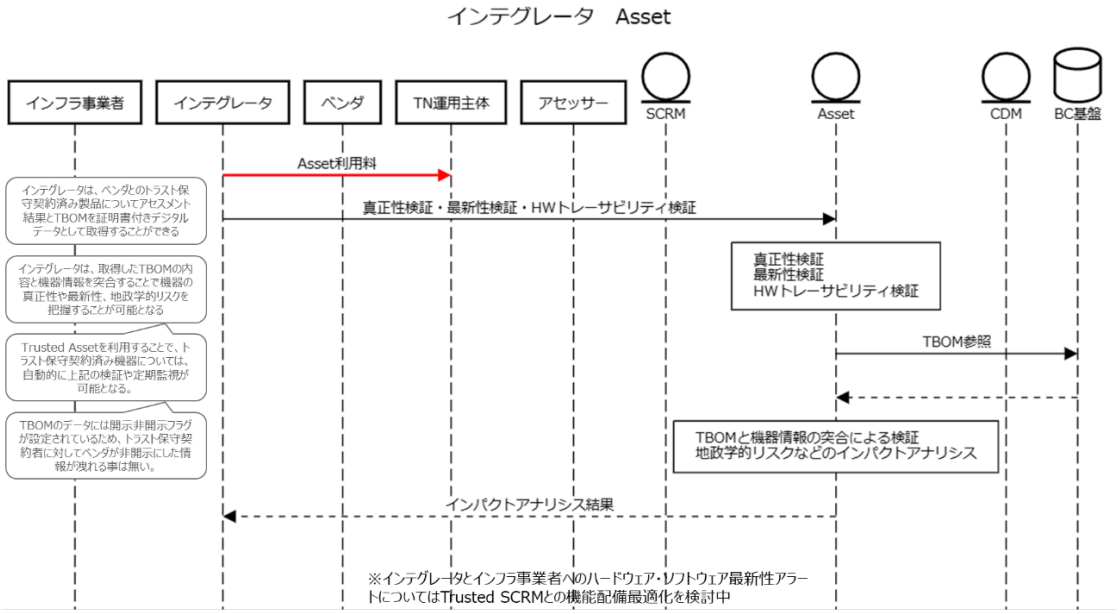


図 3.4-6 インテグレータ Asset

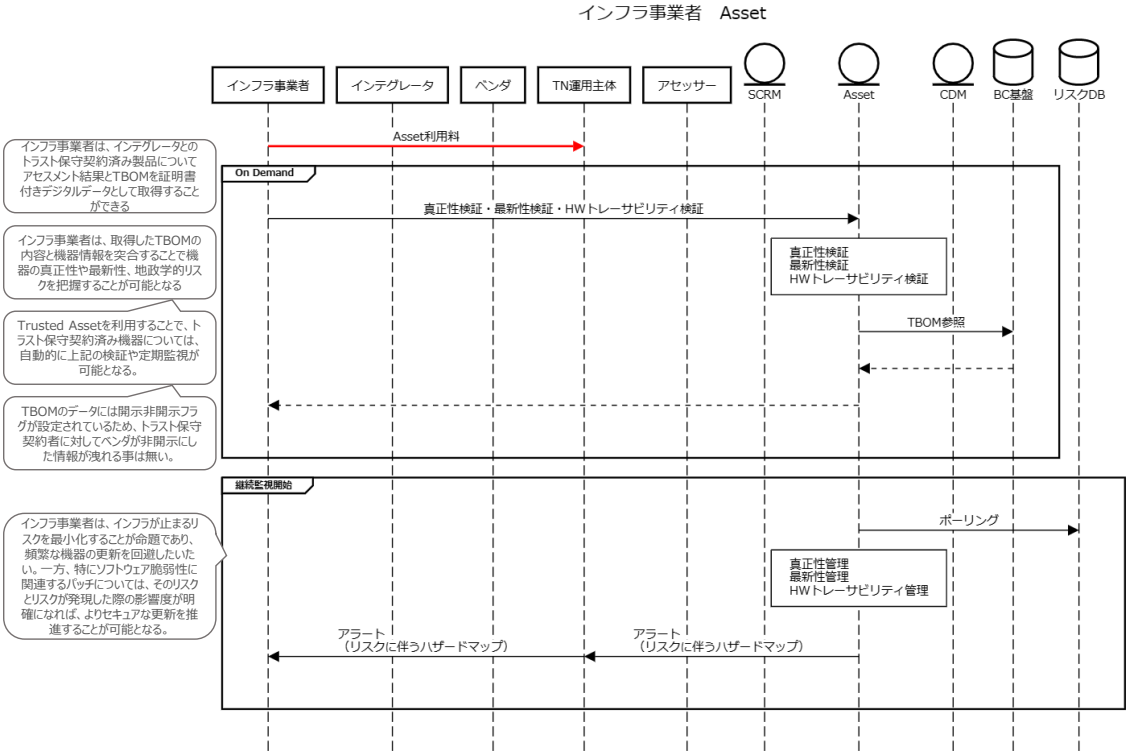


図 3.4-7 事業者 Asset

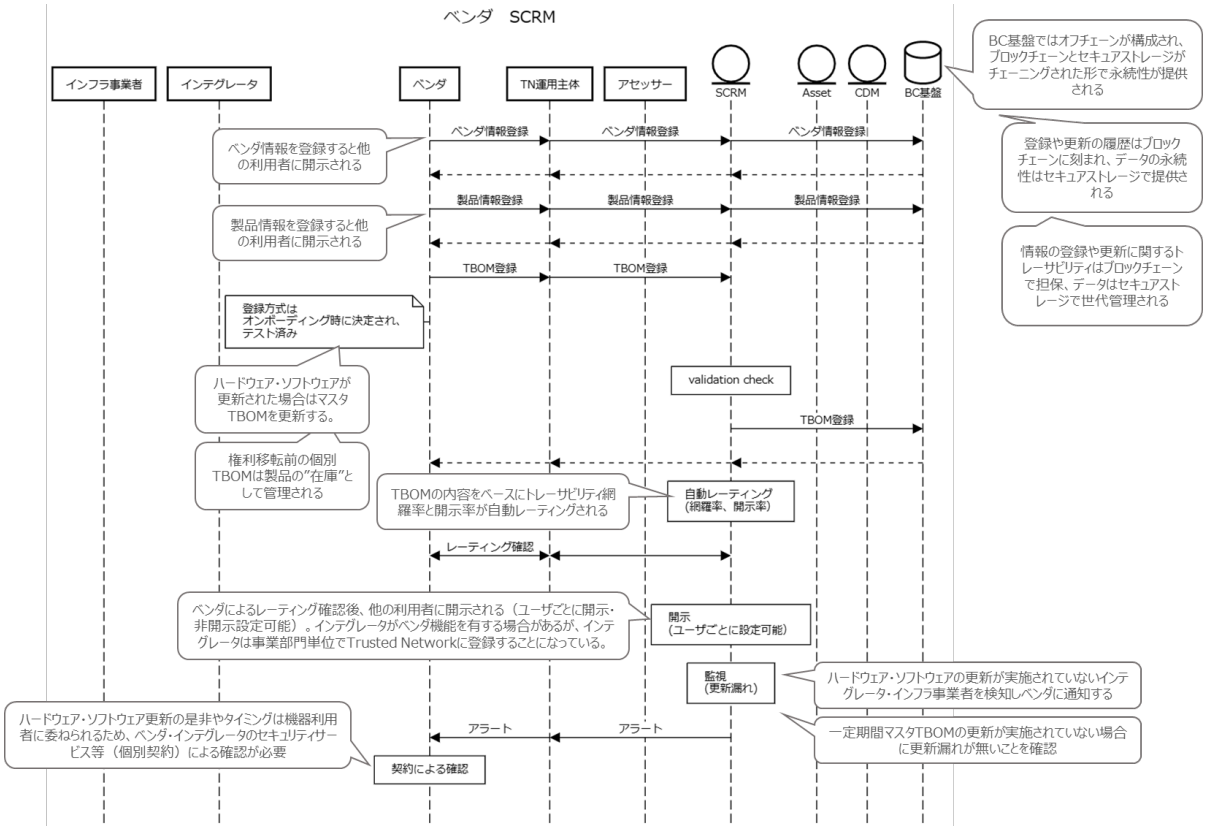


図 3.4-8 ベンダ SCRM

・Validation Check では、TBOM データが有効な値であるか、必須欄が空欄でないかなどをチェックする。

・レーティングの網羅率は、TBOM 記載対象項目をどれだけ情報提供しているか、開示率は、ベンダが TBOM に記載されたデータをどれだけ開示しているか（開示したくない情報は開示不可フラグが有効となっている）を示す。

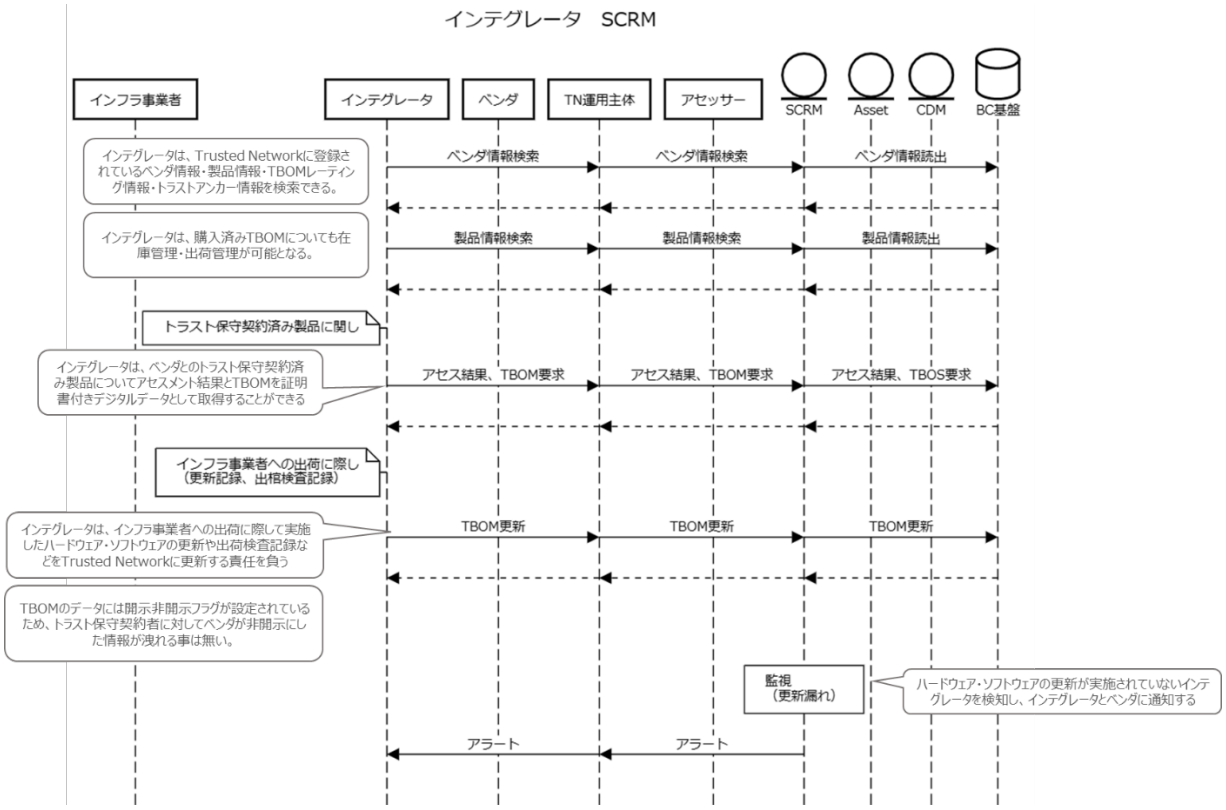


図 3.4-9 インテグレータ SCRM

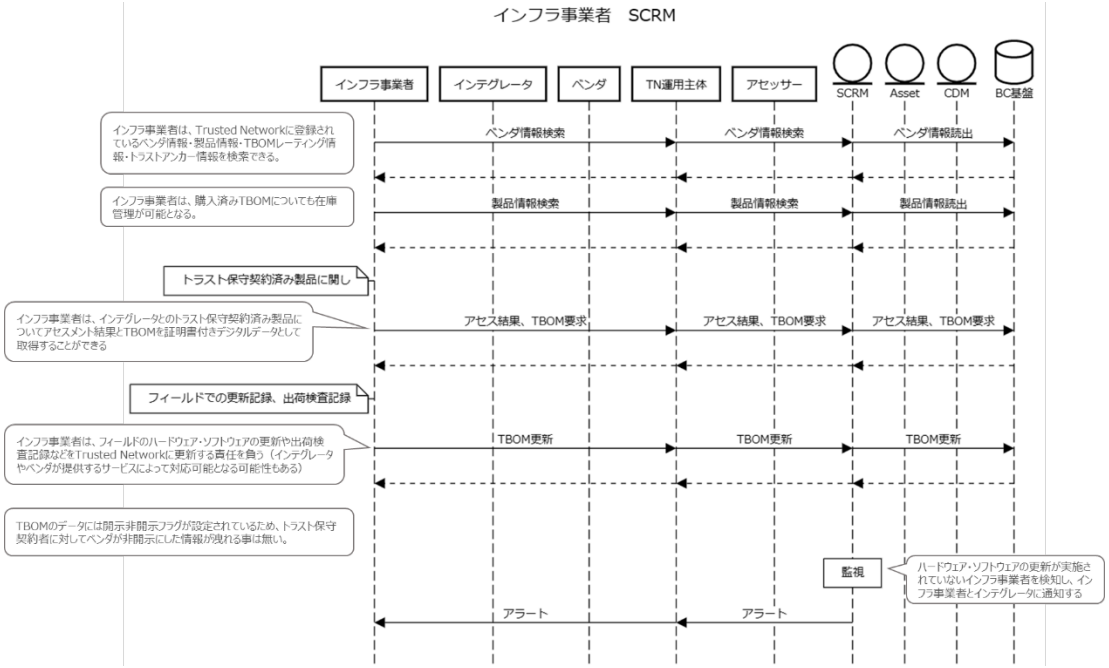


図 3.4-10 事業者 SCRM

3.4.2 業務フロー

図 3.4-1、図 3.4-2 および図 3.4-3 に TN の典型的なユースケースの業務フローを示す。

図 3.4-1 は、インフラ事業者による基幹インフラとして使用される IT 機器の調達に関して、公示、入札、受注までの業務フローを示す。
図 3.4-2 は、インフラ事業者がベンダ/インテグレータから IT 機器の調達契約をした後、出荷、構築、テストまでの業務フローを示す。
図 3.4-3 は、インフラ事業者の IT 機器運用における業務フローを示す。

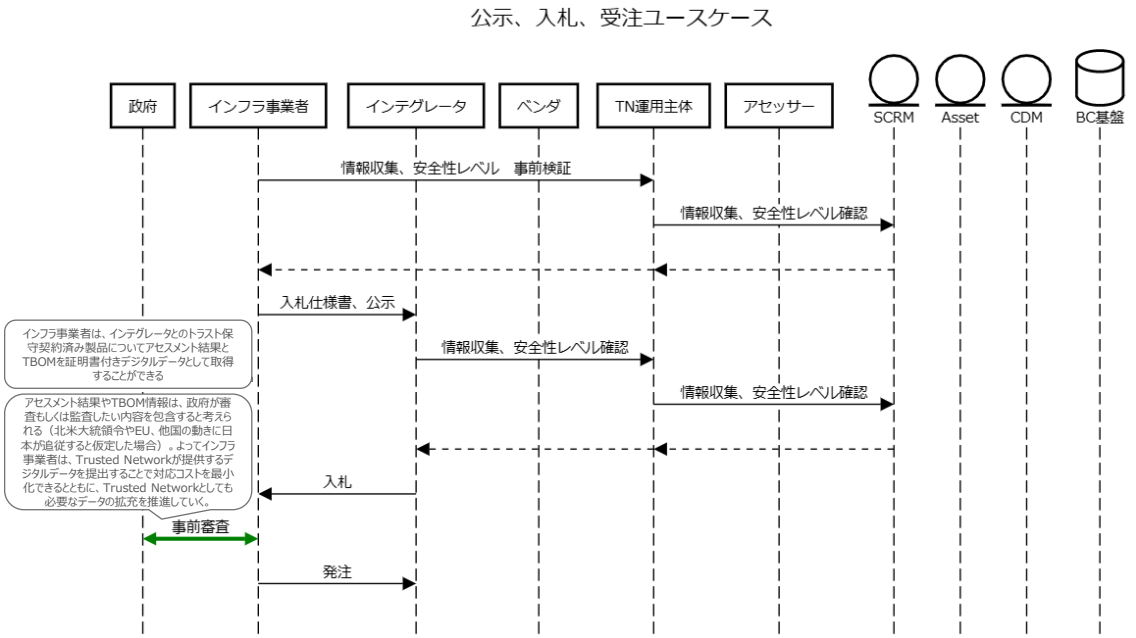


図 3.4-11 公示、入札、受注ユースケース

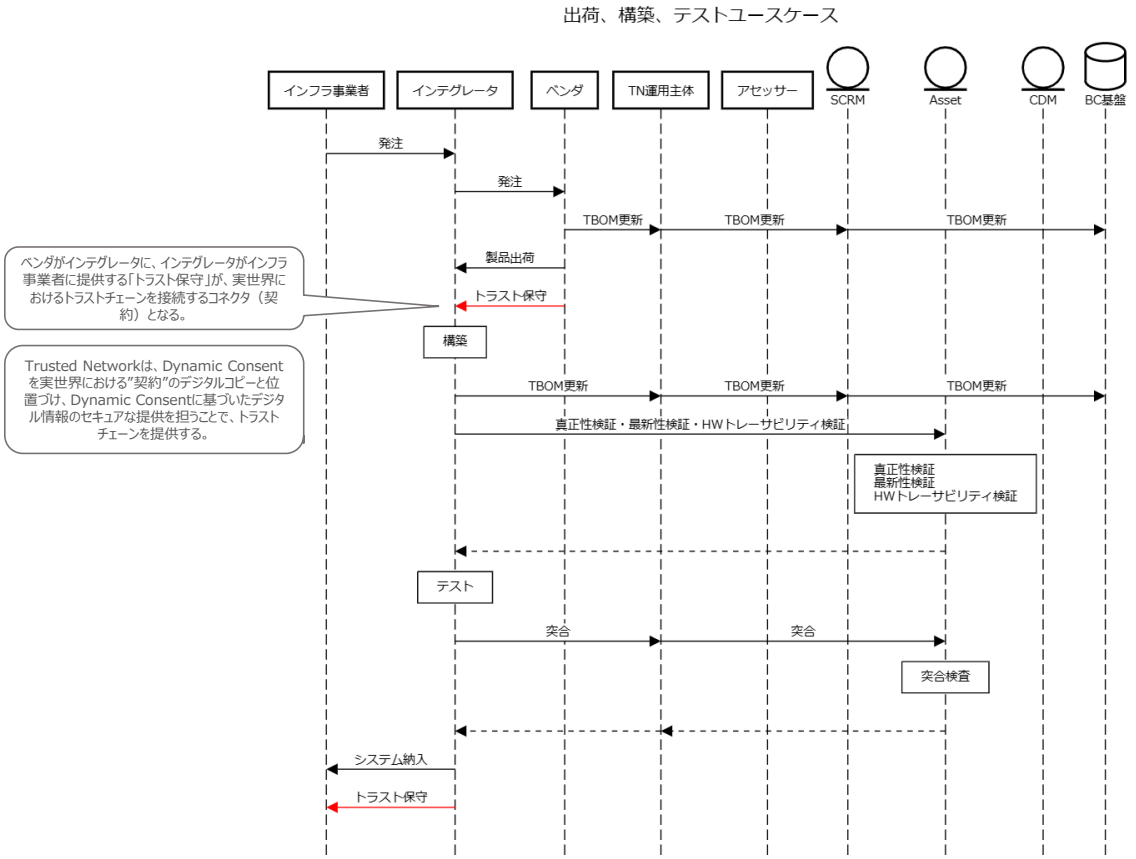


図 3.4-12 出荷、構築、テストユースケース

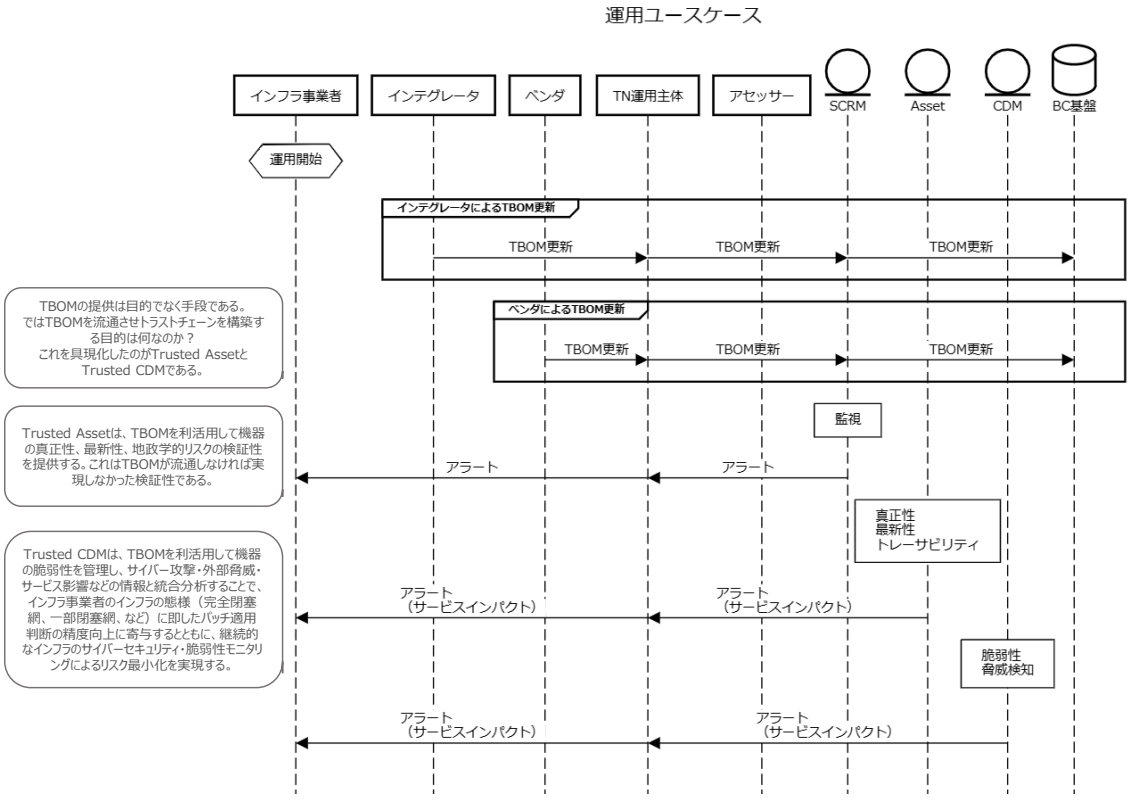


図 3.4-13 運用ユースケース

3.4.3 ユースケース図

図 3.4-4～図 3.4-10 に TN のユースケース図を示す。

（1） TNP への利用者登録

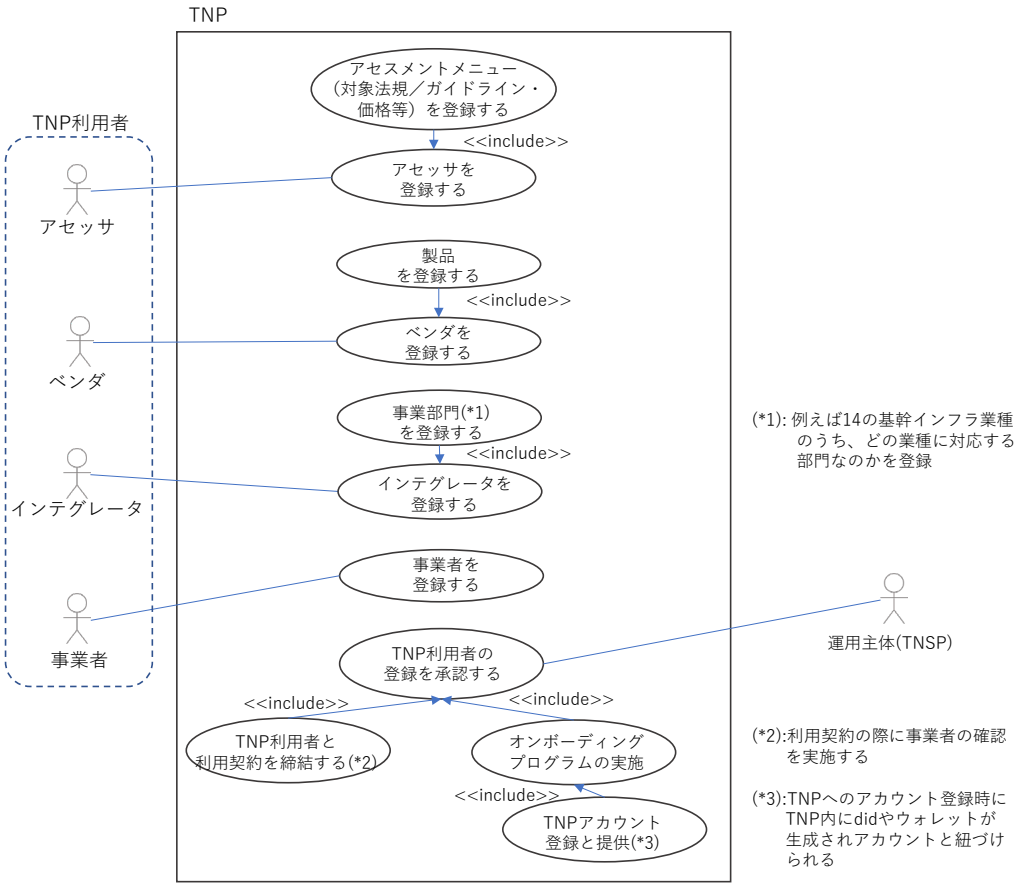


図 3.4-14 TNP への利用者登録

（２） TNP への取引先登録

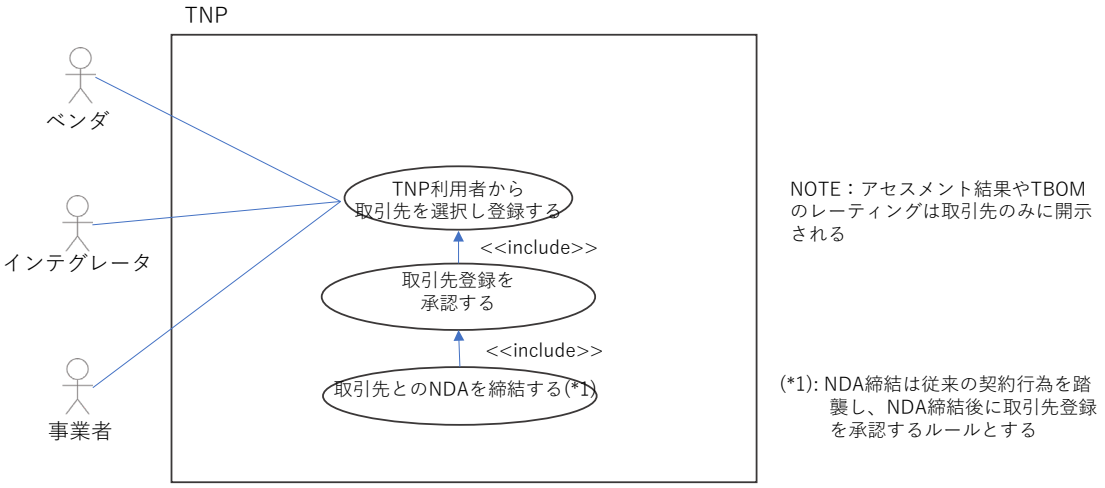


図 3.4-15 TNP への取引先登録

（３） アセスメントによるトラストアンカー コンプライアンス検証性

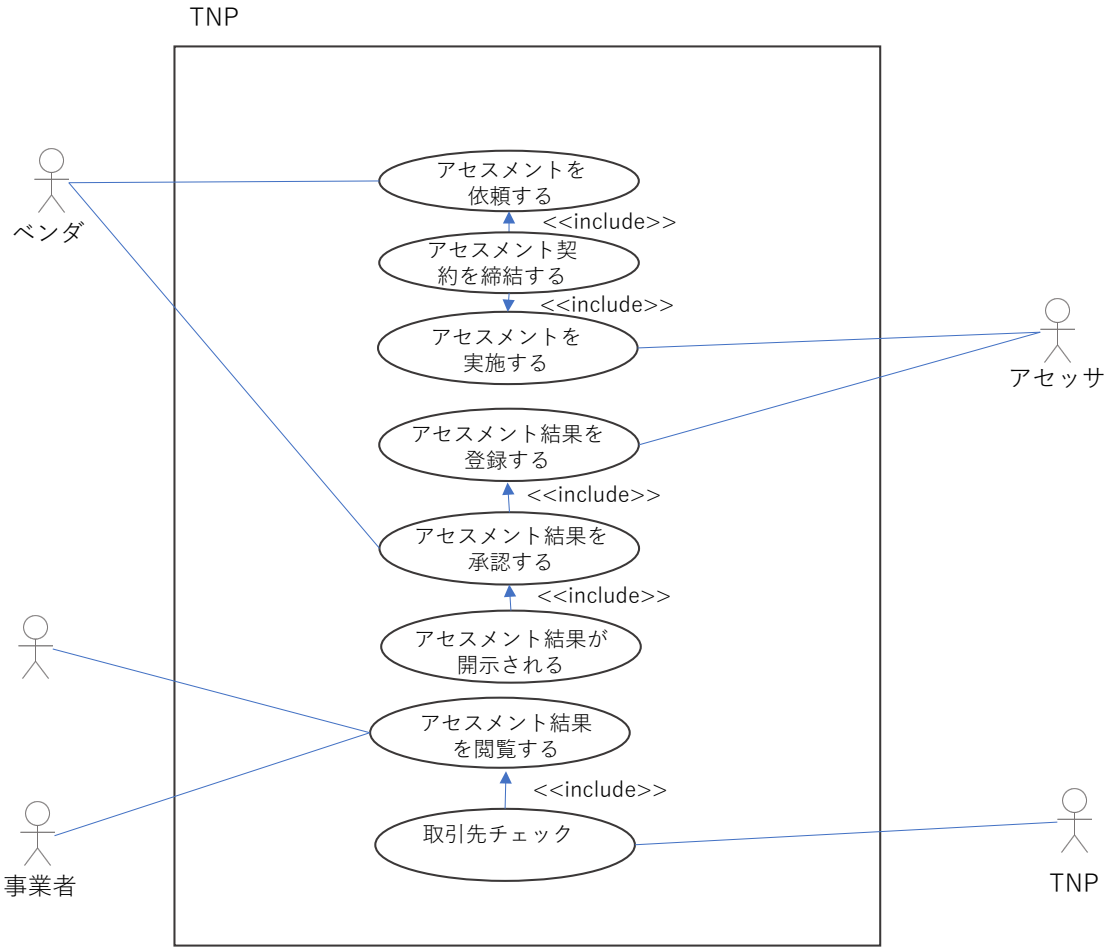


図 3.4-16 アセスメントによるトラストアンカー コンプライアンス検証性

（４） TBOM の登録とレーティング閲覧セキュリティ

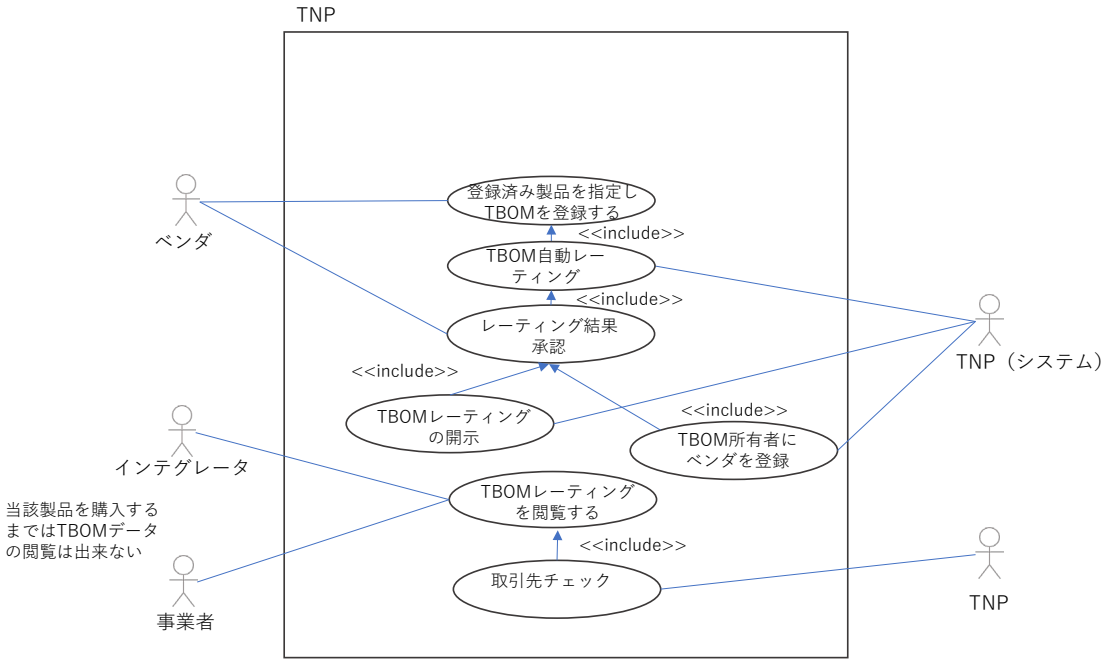


図 3.4-17 TBOM の登録とレーティング閲覧セキュリティ

（５） 契約による TBOM アクセス権の移転

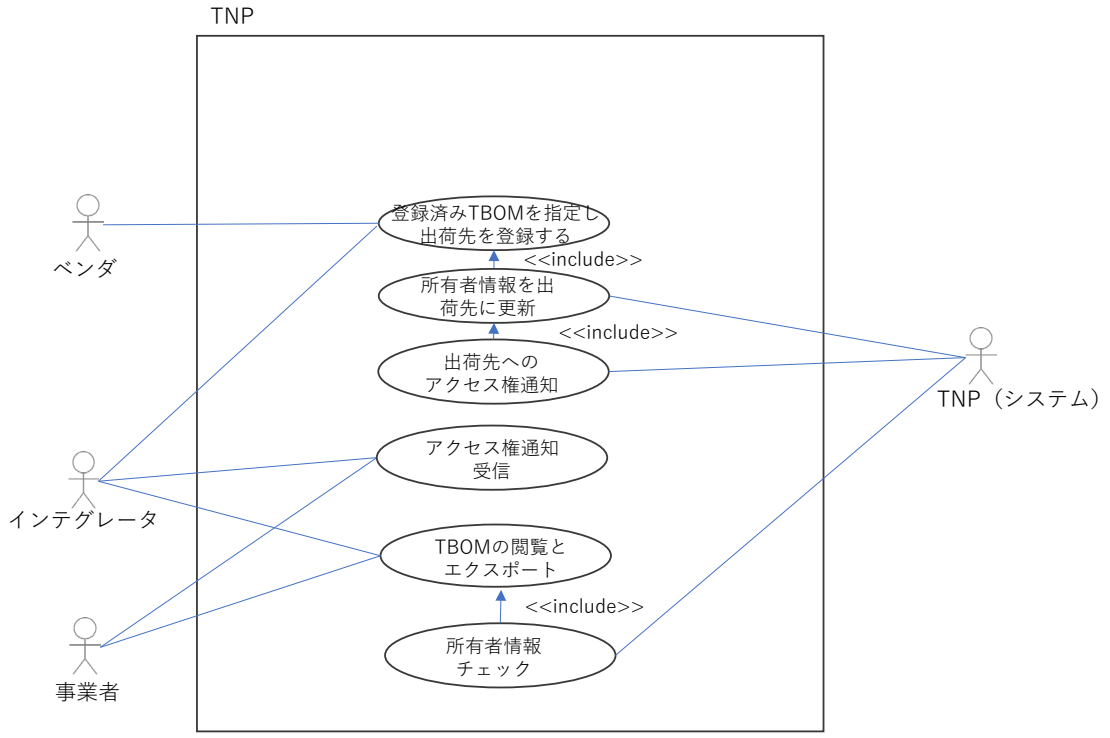


図 3.4-18 契約による TBOM アクセス権の移転

（６） TBOM アクセス権の移転と TBOM 更新

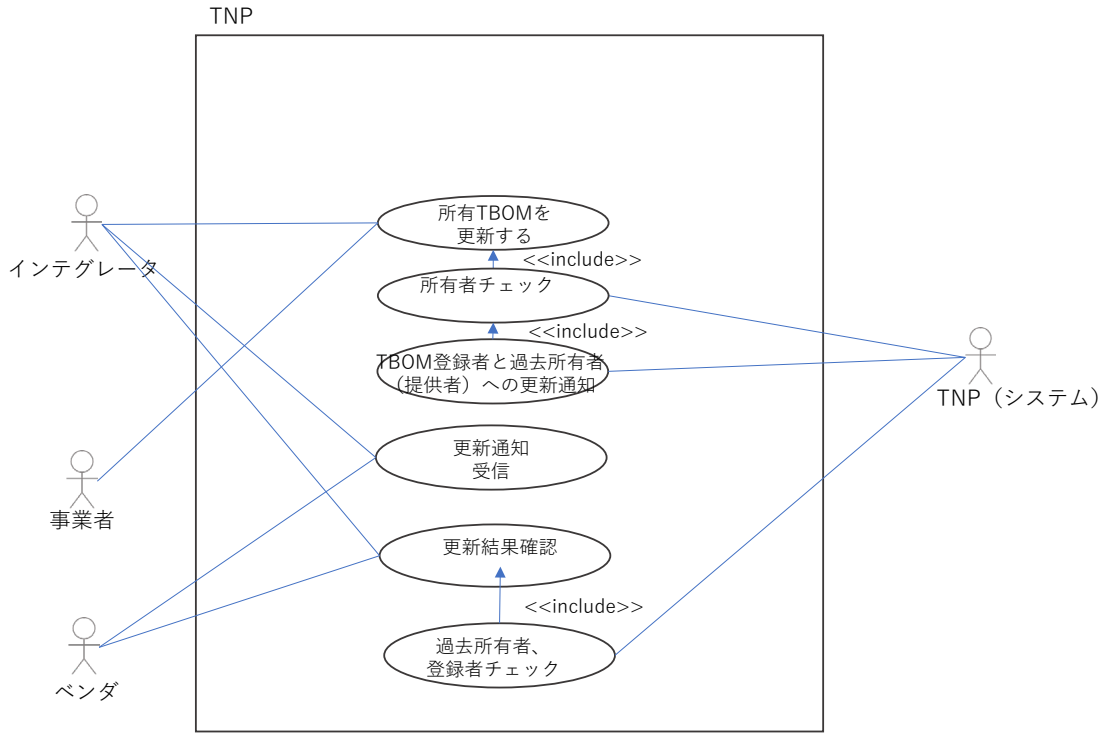


図 3.4-19 TBOM アクセス権の移転と TBOM 更新

（７） TBOM 最新情報更新

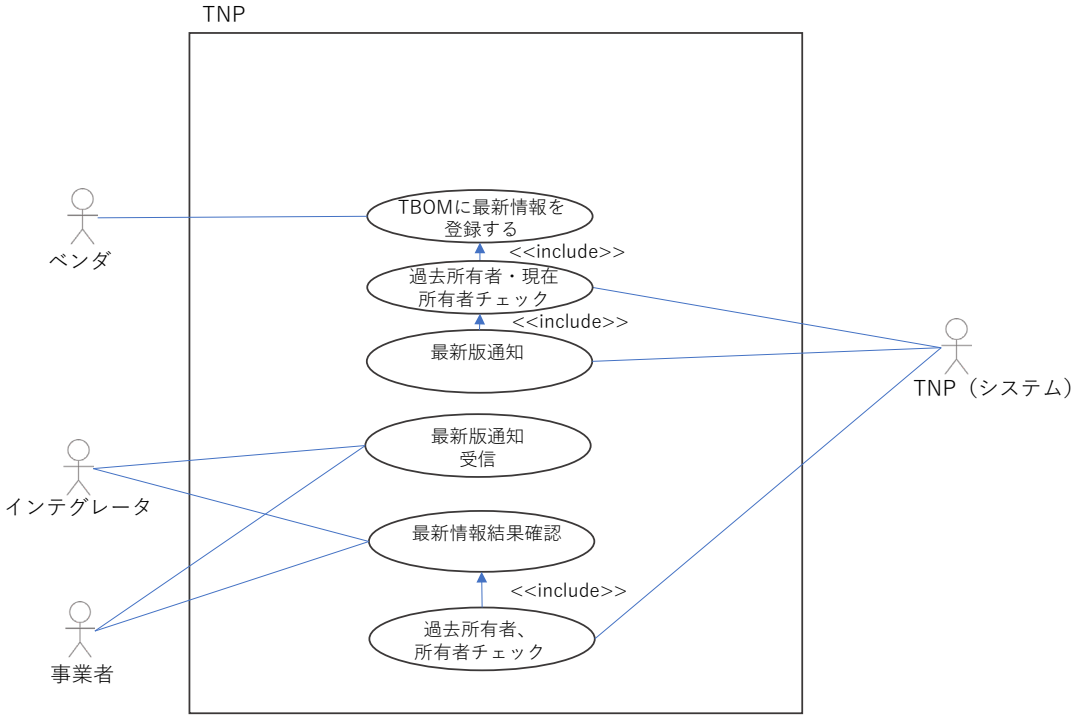


図 3.4-20 TBOM 最新情報更新

3.4.4 操作画面（UI）

操作画面については成果報告書概要版にて記載する。

またデモンストレーション動画も参照。

3.4.5 機能一覧/非機能一覧

TN は、以下の４つの機能要素からなる。このうち、Trusted Web の要件をもつ Trusted Assessment、Trusted SCRM（Supply Chain Risk Management）、について要件（求められる基本機能）定義を行った。

表 3.4-1 基本機能要素

機能要素	概要
Trusted Assessment	ベンダとインテグレータは、アセッサによる、企業としてのアセスメントを受けることができる。アセッサが、その結果を公開することで、ベンダとインテグレータの優位性や法制および調達基準への適合レベルをベンダはインテグレータと事業者に、インテグレータは事業者に訴求できる。ベンダとインテグレータは、アセスメントを通して、自社の Trusted レベルを改善することができる。 また、製品のアセスメントも受けることができる。製品の安全性・信頼性に関わるトラストのレベルとそのエビデンス（アセスメント結果）を示すことで、TN 上で流通・提供する IT 機器の信頼性を客観的に担保できる。 スコアリングの方法は、公開される。ベンダは他のベンダの情報を見ることはできない。インテグレータも他のインテグレータの情報を見ることができない。 Trusted レベル情報の社内操作による改ざん防止とデータ保全を実現できる。 アセッサは、公益的第三者(*）による認証を通じて、随時、追加される。 *: たとえば独立行政法人や政府機関などで、ISO9001, 14001, 27001 などの規格への適合審査機関を認定するような機関・団体
Trusted SCRM	IT 機器のサプライチェーン（半導体などのハードウェアの部品メーカー、OS やアプリケーション、制御ソフトウェアなどのソフトウェアメーカー、それらのカスタマイズや設定、保守など行うシステムインテグレータ、さらにそれらの下請け企業などの流通経路上のつながり）ののさまざまなリスクを事前に予測・特定・評価し、サプライチェーンが寸断しないように必要に応じた対策を計画的に実施することを SCRM（Supply Chain Risk Management）と呼ぶ。重要インフラ(定義は用語集参照)の場合、対象となるのは、製品情報に加えて、ロジスティックスのトレイルログ、契約記録、検査記録、設定ログである。

	製品に付随するデジタル情報を製品信頼情報（Trust BOM、略して TBOM）と呼ぶ。TBOM には、ハードウェア、ソフトウェアの両方を含む。それぞれ、HBOM、SBOM と呼ばれる。 ベンダは、TBOM 情報を登録する。その際、自動的に TBOM の全体における開示率に応じたスコアが付与され、閲覧するインテグレータ、事業者は信頼する情報をどのくらい管理しているか（網羅性）、どのくらい開示しているか（透明性）を評価し、調達基準と比較するなどして安全な製品を調達することを可能となる。 インテグレータ、事業者は、採用候補であるベンダの製品の TBOM を閲覧することができる。また、機器情報の社内操作による改ざん防止とデータ保全を実現できる。
Trusted Asset	事業者が調達する、あるいは調達した IT 機器に関して、 ・最新性の確認 TBOM 登録情報と製品から読み出した、H/W、S/W のリビジョン、バージョン情報より最新であるかを確認する。 ・トレーサビリティ情報の確認 各製品の TBOM 情報より、H/W（部品）、S/W（モジュール）等のトレーサビリティ情報・レーティング情報を確認する。トレーサビリティ情報としては、例えば部品/製品の認定に関する識別番号/認定日/認定結果/認定会社/住所/認定者、製造に関する識別番号/製造日/製造検査結果/会社/住所/製造者などの情報がある。 ・真正性の確認 TBOM と製品個体情報との突合により、「本物である」かつ改ざんが無い事を確認する。 機能を提供し、調達時および調達後の IT 機器の資産管理で安全性を確保するのと同時に、ゼロデイ攻撃対策の強化、製品脆弱性（CVE/CWE）※検証と掛け合わせることで製品買い替えか、継続利用（ソフトウェア、保守の更新）の合理的な選択など資産更新計画の立案を支援する
Trusted CDM	米国政府機関に適用されているサイバーセキュリティ体制強化、分析、リスク軽減を目的とした制度を、TN にて企業向けに適用できる形に拡張したセキュリティ運用管理機能。 重要インフラ事業者を含む事業者が直面する脅威の削減、サイバーセキュリティ態勢に対する可視性の向上、およびサイバーセキュリティへの対応能力の強化を目的とする。

	Trusted CDM により、 ・（セキュリティの異常を検知する）センサー配備と活性化を統合管理し、フィード情報の一元的統合 ・アーリーワーニング（早期のリスク警報）情報と攻撃検知、資産脆弱性を総合管理することで被害の最小化 ・障害発生時影響箇所の特定だけでなく影響展開を可能とし、サービス影響を意識した適切な対策を支援 を実現することができる。 Trusted CDM は、以下の機能を提供する。 ・SBOM を用いた脆弱性検知と脆弱性情報の絞り込み ・脆弱性情報のレーティングによる優先度付け ・各種連携ツール、センサーのフィード統合、ソース毎の検出条件設定による攻撃検知情報の絞り込み ・攻撃検知情報のレーティングによる優先度付け ・ワークフローを用いた、リスクの低い作業の(半)自動化（メール連絡、PC の切り離しなど）

※ CVE (Common Vulnerabilities and Exposures, 共通脆弱性識別子)は、脆弱性情報を一意に管理するための識別情報、CWE (Common Weakness Enumeration, 共通脆弱性タイプ一覧)は、脆弱性を種類別に分類した指標で、グローバルで共通な基準として定められている脆弱性に関する情報

(1) TN 機能一覧

表 3.4-2 TN 機能一覧

機能/非機能	機能名	アクター	機能概要
機能	ユーザ登録	ベンダ、インテグレータ、事業者、アセッサ、TN 運用主体(TNSP)	ベンダ・インテグレータ・事業者・アセッサは、TN 運用主体（公益的第三者）と TN 利用契約を締結し、ユーザ登録が行われる。 登録済みユーザ一覧と詳細情報は、TN 利用者全員が閲覧可能となる。
機能	製品登録	ベンダ	ベンダは、TN で TBOM を提供する製品を TN 登録済み製品の一覧と詳細情報は、TN 利用者全員が閲覧可能となる。

機能	アセスメントサービス登録	アセッサ	アセッサは、自社が提供するアセスメントサービスについてTN に登録を行う。登録されたサービスの一覧と詳細情報は、TN 利用者全員が閲覧可能となる。
機能	アセスメント依頼	アセッシ（ベンダ、インテグレータ）、 アセッサ	ベンダは、アセッサ／アセスメント一覧からアセスメントを選択、アセスメント対象製品を選択したうえでアセスメント依頼を行う。 インテグレータは、アセッサ／アセスメント一覧からアセスメントを選択、自部門のアセスメント依頼を行う。
機能	アセスメント申請受理・契約	アセッサ アセッシ	アセッサは、TN 経由でアセッシからのアセスメント依頼を受理し、当該アセッシと協議の上アセスメント契約を締結、契約に基づいてアセッサ-アセッシ間の Dynamic Consent（アセスメント結果に応じてアセッシが開示可否を動的に決定）の関係を形成する。 この時点で当該製品または自部門のアセスメントステータスは"アセスメント中"に更新される。
機能	アセスメント実施・完了登録	アセッサ アセッシ	アセッサは、アセッシとの契約に基づきアセスメントを実施、アセスメントレポートを完成させる。 完成されたアセスメントレポートは、内容確認のためアセッシに確認依頼される。
機能	アセスメント結果確認完了、開示	アセッサ アセッシ	アセッサは、アセッシから受領したアセスメントレポートの内容を確認し、問題が無ければ TN 利用者に開示する。 もし問題がある場合、アセッサと連携し問題を解消したうえで開示する。
機能	TBOM 登録	ベンダ	製品の最新構成と過去履歴を反映したマスタ TBOM と個体の構成を反映した個別 TBOM を作成、TN に登録する。TN への登録方式は、オンボーディングで合意しテストされた方式に従う。 TBOM 登録時には、TBOM に格納される情報一つ一つについて開示・非開示の設定を行うことができる（*1）。 ※登録時、TNP は validation check（有効な値であるか、必須欄が空欄でないかなど）を実施し、invalid data についてはエラーとしベンダに通知する。
機能	TBOM レーティング結果登録	TNP ベンダ	登録された TBOM の内容をベースにレーティングを実施、ベンダに開示確認を行う。 レーティング情報は下記で構成される。レーティングの根拠とエビデンスはレーティングとともに開示される。 ・HBOM レーティング

			- 使用する基幹部品毎にトレーサビリティ情報（部品形名、部品諸元、部品取引先、部品メーカ、部品生産工場など）がどのくらい管理(記録)されていて、どのくらい開示しているかに基づいてスコア化 ・SBOM レーティング - ファイル毎にトレーサビリティ情報（コピーライト情報、入手先（提供元定義）情報、 ライセンス定義）がどのくらい管理(記録)されていて、どのくらい開示しているかに基づいてスコア化 - パッケージ毎にトレーサビリティ情報（入手先（提供元定義）情報、ライセンス定義）がどのくらい管理(記録)されていて、どのくらい開示しているかに基づいてスコア化
機能	TBOM レーティング結果確認・開示可否確認	TNP ベンダ	レーティングを確認、問題が無ければ開示合意する。 問題がある場合、TBOM を更新し再登録を行う。
機能	TBOM レーティング開示	TNP	ベンダが開示に合意したことを開示内容と共に記録し、TNPF 上に開示する。
機能	アセスメント結果、TBOM レーティング閲覧（調達・選定時）	事業者	調達要件として、ハードウェア構成情報やソフトウェア構成情報の提供要否やトレーサビリティ網羅性・透明性要件、各種標準への準拠要件の扱い（必須なのか加点要素となるのかなど）を明記する。 調達要件決定時、TN のトラストアンカーや TBOM レーティングを参照することで、現状のベンダ・製品・インテグレータのトラスト実態を定量的に把握することが可能となるため、必要に応じて調達要件を調整することが可能となる。
機能	アセスメント結果、TBOM 情報の利用権付与（発注・購買時）	インテグレータ	調達要件に応じて、各ベンダの各製品について[1]TBOM 情報の有無、[2]ベンダが管理している情報の網羅性、[3]ベンダが管理している情報の開示性、[4]Trusted Assessment で提示されるトラストアンカー情報と調達要件の適合性、などを勘案し、機種選定を行う。 インテグレータは、仮に TN に TBOM が登録済みであっても、事業者の調達要件に応じて TBOM の利用／非利用を選択できる。TBOM を利用する場合、当該ベンダにトラスト保守の見積もり依頼を実施し、当該ベンダより当該製品のトラスト保守体系とその価格（原則は年契約だがベンダが自由に設定できる）を入手の上、提案に盛り込む。

（*1）TBOM の開示／非開示の設定の仕組み（今回実装した方法）

① Quorum では標準的なアクセス管理の仕組みが実装されていないため、今回は独自実装でアクセス管理を実現（本来は Trusted Web 通信機構で実現されるべきであると考えるが、Blockchain の仕組みを使ってデータを転送）。

② 上記の独自実装の仕様は以下のとおり

・TN では"論理ギャランティーカード"という NFT（定義は用語集参照）の概念を定義し、このカードに"誰が登録し誰が保全するデータか、誰がアクセス権を有しているか"の情報を記録。

・論理ギャランティーカードは製品に紐づく形で生成され、現時点の所有者証明を可能とする

・この所有者証明により権限管理を実現しており、自らが所有している、もしくは過去に所有していた製品に対して、トラスト保守を提供する主体（ベンダ、インテグレータ）は TBOM の登録や編集（更新）が可能。権限管理の仕組みは独自実装。

③ 現実世界でトラスト保守契約が成立した際、トラスト保守提供者（ベンダあるいはインテグレータ）がそれを TN に登録することで、論理ギャランティーカードのアクセス権情報を更新する（所有者を示す DID を更新し、その後は履歴をチェーンに刻む処理を行う）

④ これによって、トラスト保守契約を締結したユーザが誰であるかの履歴を改ざん不可能な形で記録しトレーサビリティを確保するとともに、現在誰がアクセス権を有しているかの情報の永続性を実装。

⑤ アクセス制御の仕組みにより、導入した IT 機器に紐づく TBOM 以外は導入者（事業者）の画面に表示されなくなる（事業者 A でログインした場合、事業者 A がアクセス権を有する TBOM だけが一覧に表示されない）。

⑥ 「論理ギャランティーカード」、「TBOM」はそれぞれ別のチェーンに記録されており、両者ともに検索性がないが、このデータへの検索性とアクセス性を提供するため、「データベース」と「ブロックチェーン」双方に記録を行っており、検索に関しては「データベース」を利用した上で、「ブロックチェーン」に対してデータに間違いがないかの検証を実施する。データにアクセスする際には論理ギャランティーカードに記録されている DID との突合を実施し、権利を有するユーザにだけデータが返却される仕組みを実装した。

(2)TN の機能（操作）プリミティブ

表 3.4-3

機能		No	操作(機能)	アクター
Trusted Assessment	Subject Of Assessment	1	アセッサへのアセスメント要求	ベンダ・インテグレータ

		2	アセスメント承認	ベンダ・インテグレータ
		3	セルフアセスメントシート入手	ベンダ・インテグレータ
		4	セルフアセスメントシート送信	ベンダ・インテグレータ
		5	アセスメント中	ベンダ・インテグレータ
		6	アセスメントレポート受け取り	ベンダ・インテグレータ
		7	レーティング設定	ベンダ・インテグレータ
		8	改善日設定	ベンダ・インテグレータ
		9	公開/非公開設定・"Done"状態へ	ベンダ・インテグレータ
		10	評価レポート一覧表示	ベンダ・インテグレータ
		11	Done 状態でのレーティング変更	ベンダ・インテグレータ
	Assessment Report List	12	製品評価レポート表示	ベンダ・インテグレータ
		13	組織の評価レポート表示	ベンダ・インテグレータ
		14	改善日設定	ベンダ・インテグレータ
		15	Assessment 評価レポートのエクスポート	ベンダ・インテグレータ
	全機能	16	全操作	事業者
Trusted SCRM	代表品番	17	代表品番の一覧表示	ベンダ
		18	代表品番の登録	ベンダ
	TBOM 登録	19	マスターTBOM の登録	ベンダ
		20	マスターTBOM 登録状況の表示	ベンダ
		21	個別 TBOM の登録	ベンダ・インテグレータ

		22	個別 TBOM 登録状況の表示	ベンダ・インテグレータ
	出荷可能製品登録	23	IP アドレス、ログイン情報の設定	ベンダ
		24	CLI によるシリアル番号の読み出し	ベンダ
		25	RFID リーダによる RFID タグ番号の読み出し	ベンダ
		26	machine_info の生成	ベンダ
		27	出荷可能製品の登録（Mint）	ベンダ
	出荷	28	出荷（Transfer）の実行	ベンダ・インテグレータ
	所有製品一覧	29	所有製品一覧の表示	ベンダ・インテグレータ・事業者
	Assessment /TBOM レーティング	30	対象製品一覧の表示	ベンダ・インテグレータ・事業者
		31	Assessment 評価レポートの表示	ベンダ・インテグレータ・事業者
		32	レーティングの設定	ベンダ・インテグレータ・事業者
		33	Assessment 評価レポートのエクスポート	ベンダ・インテグレータ・事業者
		34	トレーサビリティ評価レポート HBOM の表示	ベンダ・インテグレータ・事業者
		35	トレーサビリティ評価レポート SBOM の表示	ベンダ・インテグレータ・事業者
		36	インテグレータの組織アセスメント	インテグレータ・事業者
	パートナー一覧	37	パートナー一覧	ベンダ・インテグレータ
Trusted Asset	ダッシュボード	38	ダッシュボードの表示	事業者
		39	メッセージの表示	事業者
		40	サイクルタイムの設定	事業者
	真正性確認対象製品一覧	41	真正性確認対象製品一覧の表示	事業者
		42	真正性確認の実行	事業者

	RFID リーダーリスト	43	RFID リーダーの情報の一覧	事業者
		44	RFID リーダー情報の設定	事業者
		45	IP アドレス、ログイン情報の設定	事業者
	資産一覧	46	資産一覧の表示	事業者
		47	SBOM の更新	事業者
	Assessment /TBOM レーティング （SCRM を利用する場合は、ここでは非表示にする）	48	Assessment 評価レポートの表示	事業者
		49	レーティングの設定	事業者
		50	Assessment 評価レポートのエクスポート	事業者
		51	トレーサビリティ評価レポート HBOM の表示	事業者
		52	トレーサビリティ評価レポート SBOM の表示	事業者
		53	インテグレータの組織アセスメント	事業者
All	ログ機能	54	全操作	ベンダ・インテグレータ・事業者

表 3.4-4 非機能一覧

機能/非機能	機能名	機能概要
非機能	可用性	基幹インフラ向けのサービスとなるため 24H365D 稼働が前提であり、障害発生時に機能停止せず動作を継続することを可能とする。 今回の実装では、データの格納は分散ファイルシステムおよびブロックチェーンにて行い、ブロックチェーンサーバは最低 4 台の冗長化で運用
非機能	運用・保守性	遠隔でのメンテナンスが可能。 Git サーバから自動デプロイできるように構成し、ブロックチェーンサーバおよび API サーバのデプロイを自動化
非機能	性能・拡張性	システムの性能を確保するため、製品信頼情報(TBOM)自体はセキュア・ストレージに格納し、それに紐づく格納履歴（トレース情報）のみブロックチェーンに刻むアーキテクチャとしている

非機能	セキュリティ	情報はセキュア・ストレージに格納、DID、VC の発行、利用者情報、アセスメント結果、TBOM の登録の履歴をブロックチェーンに記録し、不正な閲覧や改ざんを防止 API サーバへのアクセスはファイヤーウォールで IP アドレスを制限
非機能	移行性	現実世界の調達モデルをそのままに適用できる仕様とすることで、適用性を上げる。
非機能	相互接続性	グローバルに広がるサプライチェーンに対して、トラストを数珠繋ぎする「トラストチェーン」を形成するため、海外、異業種のトラスト基盤との接続性を確保する（課題）

3.4.6 データモデル定義(VC データモデルを採用する場合)

TNS へのベンダ登録時の VC

表 3.4-5 データモデル定義

属性値	属性取得元	属性値（vc 内）
ベンダコード	credentialSubject	vender_code
権限	credentialSubject	user_role
企業名	credentialSubject	company
担当名	credentialSubject	name
メールアドレス	credentialSubject	email
電話番号	credentialSubject	tel
発行元	issuer	issuanceDate
発行日	issuer	issuer

3.4.7 実験環境

今回の実証で構築した実験環境を図 3.4-11 に示す。

「Trusted Network Data Platform(TNDP)」はブロックチェーンおよびセキュア・ファイルシステム（IPFS）へのアクセス（データ参照、格納、更新）を行う。TNDP と実験ネットワークはルータ AX260A で接続する。TN のフロントエンドとして、TrustedAssessment、Trusted SCRM、Trusted Asset および Trusted CDM の処理を行う「Trusted Netwrok Front-end」としてサーバを接続した。また、実証対象機器として、アラクサラネットワークス社の実機 AX8600R（ハイエンドルータ）と AX3600S（レイヤ３スイッチ）を実験ネットワークに接続した。この他に、GNS3（用語集参照）を用いて設定した仮想機器も接続した。

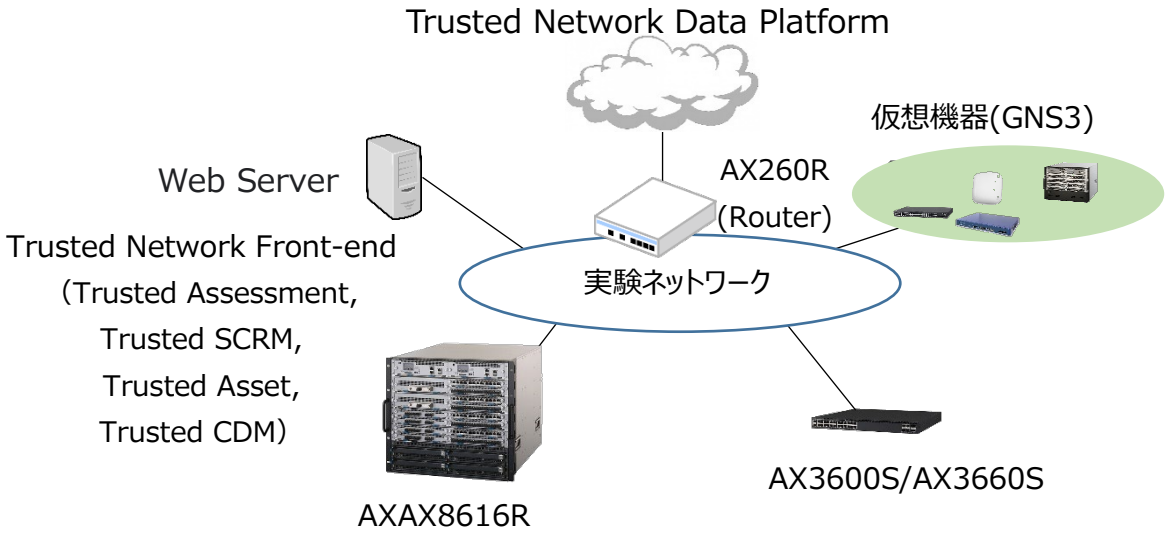


図 3.4-21 実験環境

3.4.8 システムの構成要素

システムを構成する主要コンポーネントの名称、型式、OSS の使用有無、参照する国際標準を表 3.4-5 表 3.4-6 に示す。

表 3.4-6 主要な製品・ライブラリー覧

コンポーネント名称	型式（製品の場合）	開発/流用	OSS か否か	ライセンス
Trusted Network Data platform	自社開発（型式未定）	新規開発	一部使用	–
Trusted Assessment front-end				

Trusted SCRM front-end				
Trusted Asset front-end				
Trusted CDM front-end				

表 3.4-7 参照している代表的な国際標準

#	対象	標準化機関	規格
1	DID	W3C	Decentralized Identifiers (DIDs) v1.0 W3C Recommendation 19 July 2022
2	VC	W3C	Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022
3	アセスメント	NIST	SP800-161: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
4	SBOM	Linux Foundation, ISO	SPDX (Software Package Data Exchange) ISO/IEC 5962:2021 SPDX Specification V2.2.1

3.5 実証を通じて得られた主な成果

3.5.1 システムの企画・開発に関する実証内容・得られた主な成果

Trusted Network を企画し、プロトタイプを開発、沖縄オープンラボラトリにて実機とプロトタイプによる価値実証（POV: Proof of Value）を行い評価した結果、

- Trusted Network を Trusted Web の要件を満たすシステムとして企画し、プロトタイプを実装し、実際に想定通り動作できることを実証した。
- プロトタイプの企画、開発を通じて、2.2 で述べたようなさまざまな社会課題の解決を図れる可能性があることを実証した。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

TN は、日本の基幹インフラの信頼性（Trustability）を向上させる取組みとして、公益的なプラットフォームを業界全体で協力しあって実現するエコシステムによって形成する。

そのため、TN のプラットフォームの運用主体（TNP）は、必要最低限の費用で運営し、利用者から参加費や製品信頼情報（TBOM）の登録・利用料、さらにオプションサービス（脆弱性管理、早期警戒等）の料金を徴収するマネタイズ手法を検討した。

沖縄オープンラボでの価値実証では、ビジネスモデルに関して TN-PJ メンバからのフィードバックとして、以下のような意見が得られた。アンケート結果によるものなので、詳細な背景、理由までは把握できていないが、概ね社会的価値はある、あるいは改善次第で価値を出すことは可能との意見が主であったが、価格については想定した価格（＊１）では高いとの意見や、価値を十分理解できていない/明確化できていないため価格の妥当性評価が難しいといった評価となった。

（＊１）機器の価格の２%を年間のトラスト保守料として事業者から徴収する想定とした。IT 機器の年間保守料が一般に機器価格の 10%程度であることから、事業者のトラストを維持するコストとして上記 2%を暫定値とした。また、TN の利用料としては国内の重要インフラを提供する上位５～１０社（年間売上数千億～数兆円クラス）に対して、1 社あたり年間 360 万円を想定した。

3.6 本実証で開発したシステムの第三者による再現可能性

第三者が、同様なシステムを本報告書に記載した機能要件に基づいて再現することは可能と考える。

本実証では、アラクサラはプロトタイプの開発をすべて自社費用で実施した。開発投資は数億円以上に及ぶため、同様なシステムの開発を個社で行うのは容易でない。

個々に投資をするくらいなら、先行する TN エコシステム構想に参画して、共創していくほうが、コスト的にも、複数方式並立による混乱をさけるためにも、望ましいと考える。

また、国内で同様なシステムを併存させ、「競争」で磨き上げていくアプローチでは、諸外国でのサプライチェーンにおけるトラスト確保のシステム化や標準化の速い動きに追従できず、結局は日本として諸外国の方式に合わせざるを得ないことになってしまうことが危惧される。

なお、TN の基本的なコンセプト、方式、設計、知財は、今回の受託の前から検討・考案済であった。今回の実証事業では、TN の基本コンセプトと Trusted Web のコンセプトとの共通化を図る見直しを実施した。

4　実証終了後の社会実装に向けた見通し

4.1　社会実装時に想定しているビジネスモデル・ユーザーのメリット

図 4.1-1 に TN のビジネスモデル、表 4.1-1 に TN ステークホルダごとのベネフィットと負担コストを示す。

アラクサラネットワークスは、図 4.1-1 において TNE として TN の開発および技術提供を行うのと同時に、ベンダとして TN 利用者として参加することを想定している。

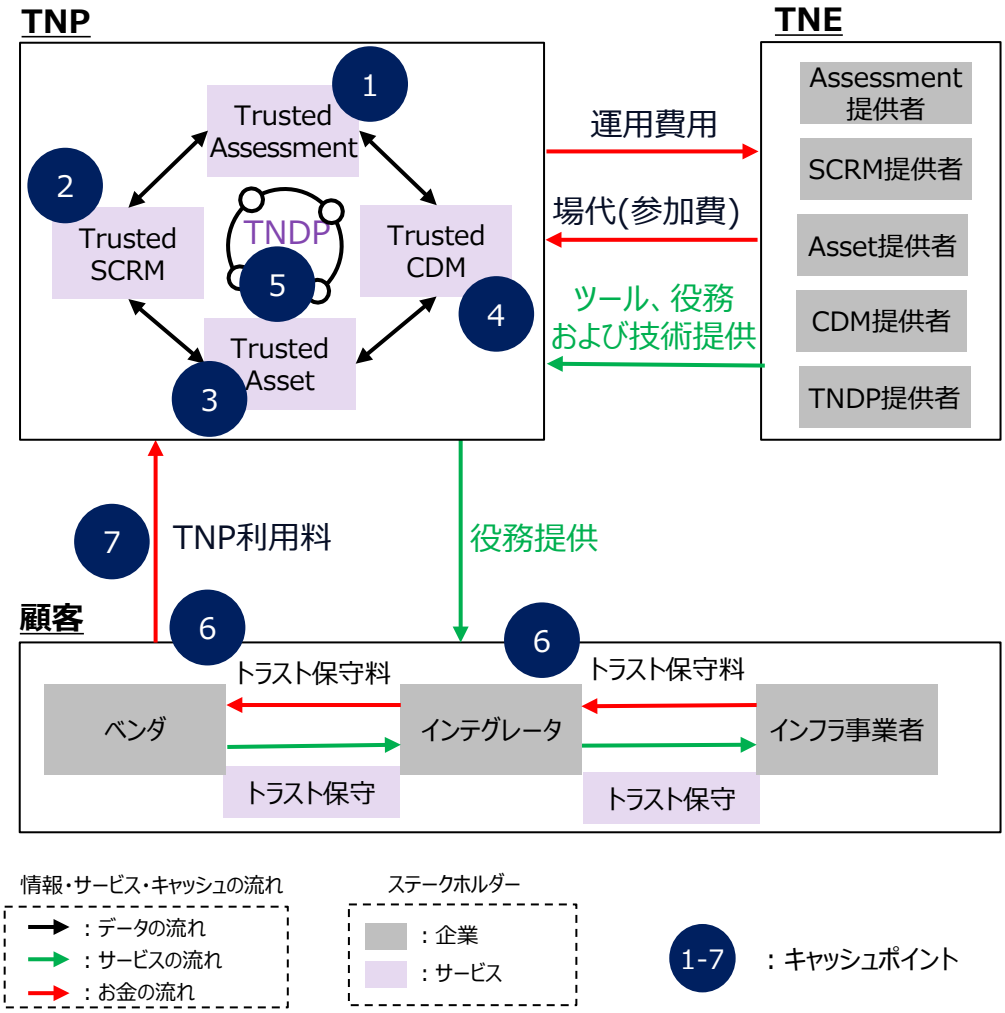


図 4.1-1　TN ビジネスモデル

表 4.1-1 TN ステークホルダごとのベネフィットと負担コスト

ステークホルダ	ベネフィット	負担するコスト

TNSP (TN の運用主体。公益的第 3 者)	日本の IT インフラの信頼性向上（公益）	• オンボーディング費　(デジタル ID 付与) • トレーニングに関する費 • サービス・システムの維　持・メンテナンス費
事業者	信頼性のある（トラスタブルな）製品調達 経済安保推進法対応	• オンボーディング費 • 利用登録費 • TN 利用費 • トラスト保守費 • TBOM の維持・運営費
インテグレータ	信頼性のある（トラスタブルな）製品調達（重要インフラ顧客獲得）	• オンボーディング費 • 利用登録費 • TN 利用費 • トラスト保守費 • アセスメント費
ベンダ	重要インフラ顧客獲得 トラスト保守による収益化	• オンボーディング費 • 利用登録費 • TN 利用費 • アセスメント費
TNE (TN Enabler)	TN のサービス収入	• オンボーディング費 • 利用登録費 • TN 利用費 • トラスト保守費 • TBOM の維持・運営費 • 技術・ツール費

課金モデルとキャッシュポイント

（1）TNP 利用料は、コスト（開発・運営）回収を行う必要があり、顧客に対して一定額の費用を継続して得る料金体系にする必要がある。顧客の予算獲得のハードルも下げる必要がある。また、サービス利用料は Back to Back を想定した料金形態あり、各 TNE が提供するサービスの料金形態と平仄を合わせる必要がある。

（2）TBOM は、コスト（運営）及び利益を上乗せした金額であることと、製品単価の不透明さを加味した料金形態が必要である。また、ベンダの値段設定が高いと、インテグレータはコストと利益を乗せることで、インフラ事業者の負担が大きくなる。

（3）場代は、TNP（マーケットプレイス）を通じて、利用者と TNE をマッチングさせる事が可能となり、TNE はニーズ探索及び個別でアプローチする工数が削減される事で効率的に営業活動が可能となる。現状のコスト回収を行う必要がない為、TNP 運営主体としては、大きな収入源となる想定。TNP 運営者の安定的な収益と利用者の予算化の容易さを加味した課金形態にする必要がある。

表 4.1-2 キャッシュポイント

<table>
<tr><th rowspan="2">No.</th><th colspan="2" rowspan="2">キャッシュポイント</th><th rowspan="2">支払元</th><th rowspan="2">支払先①</th><th rowspan="2">支払先②</th><th colspan="2">回収コスト</th><th rowspan="2">TNP運営者
利益</th></tr>
<tr><th>開発</th><th>運営</th></tr>
<tr><td rowspan="2">（1）</td><td rowspan="2">PF利用料</td><td>基本利用料</td><td rowspan="2">ユーザー企業
- ベンダー
- インテグレーター
- インフラ事業者</td><td rowspan="2">TNP運営主体</td><td>-</td><td>○</td><td rowspan="2">○</td><td>中</td></tr>
<tr><td>サービス利用料</td><td>TNE</td><td rowspan="3">-</td><td>0
Back to Back</td></tr>
<tr><td rowspan="2">（2）</td><td colspan="2" rowspan="2">TBOM</td><td>インフラ事業者</td><td>インテグレーター</td><td>ベンダー</td><td rowspan="2">○</td><td rowspan="2">製品価格のX%を
Trust保守料として想定
（一般的な保守は3%程度）</td></tr>
<tr><td>インテグレーター</td><td>ベンダー</td><td rowspan="2">-</td></tr>
<tr><td>（3）</td><td colspan="2">場代（出店料）</td><td>TNE</td><td>TNP運営主体</td><td>-</td><td>高</td></tr>
</table>

4.2 実証を通じて判明したユースケースの課題とその解決方針

表 4.2-1 実証を通じて判明した課題と解決方針

#	実現上の課題	対応方針/対応状況
1	BOM 開示と委託先との合意形成の加速材料が少ない	サプライチェーンの末端までカバレッジを上げること価値は少なく、まずベンダがトレーサビリティを直接担保できる範囲にスコープを絞って価値訴求する
2	実世界と Web 3.0 世界のビジネス形態の整合	実世界の調達にインパクトしない導入を最優先事項としてアーキテクチャやオペレーションの設計を実施する。
3	色々なサプライチェーンセキュリティの取組の統合に手間と時間がかかる	既に対話を始めているが、足りない所を補完し合う形で統合を進めていくよう協調・共創型の取組みを推進する
4	主要国とのサプライチェーンセキュリティ政策との連携	北米や台湾など主要な地域においてはキーマンとの対話を開始、沖縄オープンラボの価値実証 PJ を活用してリレーションを強化していく

5	TN を管理・運用する主体（組織体）の立上げ	TN を管理・運用する「公益的な第三者」はどのような組織体であるべき/参画しうるか、整理する。 アーキテクチャや仕様上の課題ではないものの、実現にあたっては信頼できる組織体である必要があり、国・公共機関あるいは、その支援/介入が必要と考えている。
6	TN に格納された機器の TBOM 情報と実際の機器との間で突合を行う際、どこまで厳密な対応を実装するか	機器の真正性、所有権の検証において、機器(部品)の識別に用いる情報として[1]機器のシリアル番号、[2]搭載ソフトウェアの hash 値を用いることを要件としているが、[2]を実装している機器は少ない。 また、[1]の対策として機器に貼付する IC チップの読み取りによる対応でセキュリティ強度向上はできるが、完全ではない。一方で、どのくらいのコスト（負担）が受容できるか（ベンダ、インテグレータ、事業者）により、実装手段が変わってくる（セキュリティとのトレードオフ）ことを踏まえ、選択肢を提示する。 詳細は付録 7 (1)参照。
7	DFFT と合わせて TN のようなスキームの国際標準化 例）国を跨ぐ Dynamic consent やデータ／属性の流通を可能とする規準の作成	TN におけるデータのやり取りは Dynamic consent に応じたデータの開示／非開示をコントロールするため、一旦 TN 基盤内にデータを登録して永続性をサポートし、データへのアクセス権を移転させることで実現しており、通信プロトコルでの実現とはなっていない。どのレベルで標準化・相互接続を実現するか対応を検討する
8	TN の経済的価値と利用者（ベンダ、インテグレータ、事業者）の利用料、ベンダ・インテグレータの提供するトラスト保守の価格が事業者に受け入れられる水準の設定	TN-PJ による TN の価値実証を通して、TN の利用料・トラスト保守の価格は高いとの反応があった。提供価値（経済的価値）を十分に納得いくレベルまでにはなっておらず、妥当な価格設定が見いだせていない。単価は利用者がどれだけ獲得できるかの事業規模にも依存するところであり、今後も事業計画と価格水準についてはさらに検討していく。

4.3　本ユースケースの社会実装に向けたマイルストーン

図 4.3-1 に TN の今後の社会実装に向けた計画を示す。本ビジネスモデルの社会実装については、令和 5 年度に国際的な価値検証・接続検証を行い、令和 6 年度以降の商用化を想定している。主な課題として前述の課題⑤については、令和 5 年度にグローバル・サプライチェーンを形成する米国や台湾といった国々との価値検証を実施に取組むべく、関係機関と交渉中である。令和 6 年度のサービス開始当初は、重要インフラ市場の中でも特定の分野（例：情報通信、電力）への展開を想定しているが、令和 7 ～ 8 年度以降は他業界をターゲットにマーケティングを行い、市場の拡大を目指す。

TN は、通信ネットワーク機器をはじめとする IT 機器、産業等向けの制御システム（いわゆる OT 機器（Operation Technology 機器））および IoT 機器など、日本の社会インフラに用いられる IT/OT/IoT 機器の市場、さらにはその部品である半導体、ソフトウェアの市場にもターゲットの裾野が広がる。また、今日の IT/OT/IoT サプライチェーンは一国にとどまることはないため、半導体生産大国である台湾や先進のプロセッサ、ソフトウェアの設計、生産、販売の中心である米国にもつながっている。
こうしたさまざまな業種、国まで対象とすることができれば、巨大な市場が視野に入る。

事業展開は、まずは国内の重要インフラ事業者を初期ターゲットとして、次に国内の他事業者にも適用拡大していき、並行して各国との連携や国際標準化を進めていくことで、海外にも展開していくシナリオが現実的と考える。国内の重要インフラへの適用は、経済安全保障推進法、海外の同様な安全保障やサプライチェーンセキュリティに関わる規制（たとえば米国の大統領令による政府調達における SBOM 提出の必須化など）の程度に影響される部分がある。

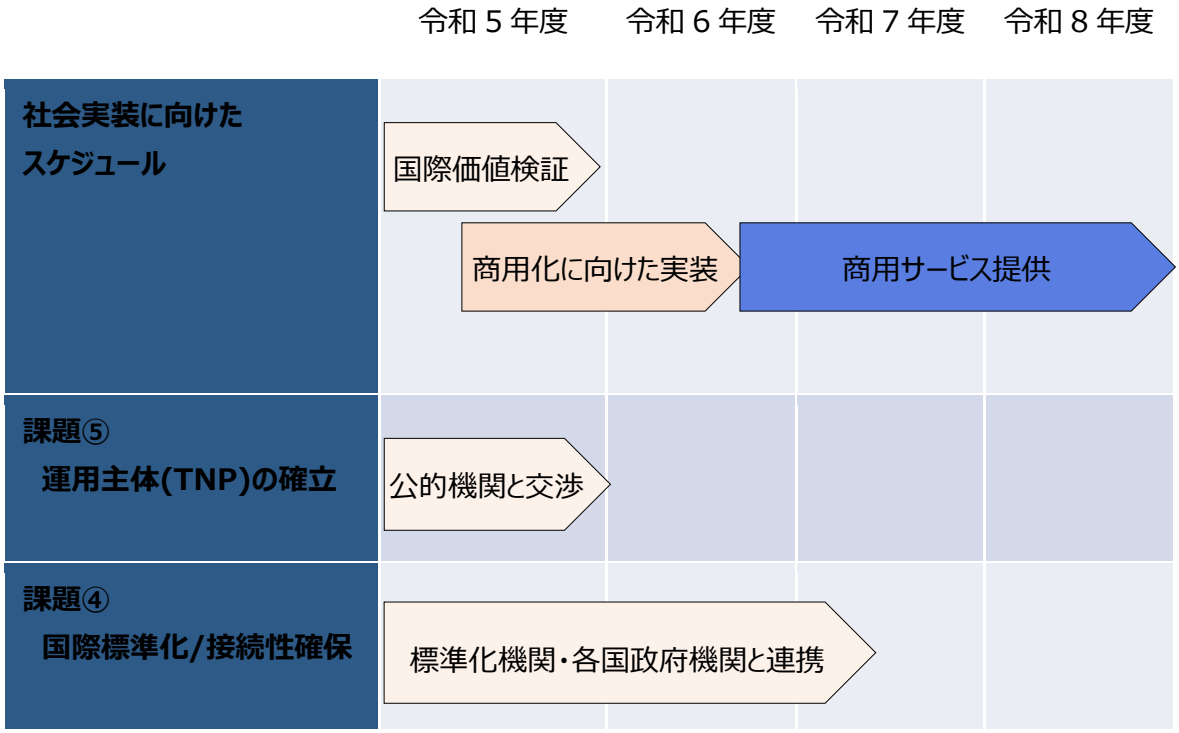


図 4.3-1 社会実装に向けたマイルストーン

5　Trusted Web に関する考察

5.1　Trusted Web のアーキテクチャに関する課題と提言

5.1.1　実装アーキテクチャの具体化

（１）　現状認識と課題

Trusted Web の実装アーキテクチャやディプロイメント設計についてもう少し具体的な記述をしたほうが良いと考える。

例えば、「データのやり取りは必ずしもインタネットを介するとは限らない」という Trusted Web における所与な要件に対し、Trusted Web はどのプロトコルにどのような形態でオーバレイされる形になるのか。

Trusted Web ホワイトペーパー 2.0（以降 TWWP 2.0）では、「Trusted Web は基本的にセッション層である 5 層以上に関するアーキテクチャであり、トランスポート層（4 層）も通信効率を上げるために検討する可能性がある」という記述があるが、これは読み手、特に実装アーキテクチャと配備設計を担当するエンジニアにとって理解しづらく、混乱を生じさせる可能性がある。すなわち、トランスポート層に手を入れる、いわゆるレイヤ・バイオレーションを実装に組み込むと、非オープンな実装となり、他業界や他国との相互接続に支障をきたすことが考えられる。

Trusted Web の実装の自由度、既存実装への適合を意識して、ホワイトペーパーでは敢えて具体化していないものと捉えているが、現実的なディプロイメントを進めていく上で、複数の OSI 層にまたがった形のシングルオーバレイプロトコルとするのか、目的や用途に応じた複数のオーバレイプロトコルとするのかといった指針を示していくべき段階に来ていると考える。

そもそも Trusted Web の要件を考えれば、データプレーン単独で実装するのは困難であり、それを考えればプロトコルの実装アーキテクチャや提供形態は自ずと固まってくるという側面がある。

データプレーンとそれを制御する制御プレーンの分離と連携や、通信の原始性保証要件とそれを実装するアーキテクチャについて言及するなど、実装設計へのガバナンスを"もう少し"効かせる段階にあると考える。そうしないと各ユースケースの実装設計が統制されず、ネットワークという本来相互接続やメッセージングを必要とするシステムにおいて、多方式乱立事態を集約するためのコストが懸念材料になりうると考える。

TN PJ においては、TN におけるデータプレーンと制御プレーンの実装設計が Trusted Web のそれと乖離し独自化することを最も懸念しており、近く決定される Trusted Web 標準仕様とそれを実装したコンポーネントの利活用を前提に、TN における各実装コンポーネントの粒度設計や凝集化設計、結合度設計を行っているが、「Trusted Web は基本的にセッション層である 5 層以上に関するアーキテクチャであり、トランスポート層（4 層）も通信効率を上げるために検討する可能性がある」というインプットに適応し続けるのはコスト的負担（特に能力的負担）が厳しい。

（２）　示唆と提言

Trusted Web ホワイトペーパー2.0 に以下のような記述を追加していくべきであると考える。

「Trusted Web プロトコルは、アプリケーション層にオーバレイするステートフルなプロトコルであり、実装形態は現段階では規定しない。Trusted Web プロトコルは dynamic consent に基づいてデータの送受信を制御する制御プレーンと、制御に基づいてデータを送受信するデータプレーンに分離実装されることを想定するが、各プレーンのプロトコル及びその実装については現段階では規定しない。」

5.1.2 検証性に関する方針の明確化

（１） 現状認識と課題

Trusted Web では、Sender と Receiver がデータをやり取りする際の検証可能領域の拡大を要件としているが、実際にデータをやり取りする前の段階でのトラストの検証と、データをやり取りした後の段階で、そのデータをアップデート（変更）した場合の検証性を提供について、明確な記載がない。

例えば、「やり取りしたデータに誤りが見つかった際の是正の仕組み」はデータのやり取りの信頼性を担保するために重要なファクターとなる。データが永続性を持つ以上、データの信頼性や検証性も永続的に提供されるべきであり、やり取りする瞬間に限定してトラストを高めるアプローチは必要十分とは言えない。

TN では、やり取りしたデータについて、受信者が永続的に利活用するユースケースを前提としているため、データ更新の有無が受信者に伝達される仕組みを実装した。換言すると、TN では同一データの更新についても永続的にトレーサビリティを提供する、即ち単位データのライフサイクルへのトレーサビリティに関する「事後検証性」を提供することを要件としており、この要件が満たされない限り、送信者と受信者に対して社会的価値と経済的価値を十分に生み出せないのでは無いかと考えている。

また、データの送受信をする前段階においても、データへのトラストアンカー（アセッサによるアセスメントで信用するに足るとお墨付きを与えること）の有無やデータ自身の透明性に関する「事前検証性」を提供することで、トラスタビリティ（価値）が高まると考える。

（２） 示唆と提言

Trusted Web における検証性の拡大が、「事前検証性」や「事後検証性」を包含するのかしないのか、包含する場合はオプションなのかマンダトリーなのか、方針を明確に示しておくべきと考える。これは今後の実装に影響を及ぼす事項となる。

5.2 その他 Trusted Web の課題と提言

5.2.1 ビジネス

（１） 現状認識と課題

Trusted Web に限らず、品質はコストであり、トラストは品質の一部である。故に、トラストはコストであると捉えられる。

Trusted Web の実装にかかるコスト、そして運用にかかるコストは誰がどのように負担するのか、また、そのコストは Trusted Web が Data Sender と Receiver の間に提供する経済的価値とトレードオフす

るのかが、Trusted Web ホワイトペーパー 2.0 では、このビジネス及び持続性の課題について、フルオープンである。

Trusted Web のような共通的な仕組みを利用することで分割損を極小化しコスト最適が実現し得ることは明確だが、それはニーズが must to have まで上がった時点で正しい。Trusted Web を利用したデータ流通が一定の経済的価値を生み出すことが前提になっているが、元々無償であったデータトランザクションにコストが発生した際、その経済的価値とのトレードオフやスケール性によって有意性が左右されるような形態は回避したい。

（２） 示唆と提言

現段階でユースケースを限定することは不可能であり、現段階でユースケースについて何らかの前提を示すことの是非について整理が必要ではあるが、利用者に対してある程度のコスト感をインプットしつつ、適用可能なインセンティブモデルやビジネスモデルの検討・共有に着手すべき段階になっていると考える。

5.2.2 政策とグローバリゼーション

（１） 現状認識と課題

今や国を超えないデータ通信のほうがレアと言っても過言ではないほど Sender と Receiver のグローバル化が進行している。仮に Sender と Receiver が隣の席に座っていても、この二者のデータのやり取りは国を超えている可能性も大いにあり得る時代である。

Trusted Web がどのように国際的な合意を形成し、実装を経て実用ステージに向かっていくのか、もう少し具体的なロードマップが示されないと、検討するユースケースや実装の範囲が制限されてしまう。

Trusted Web の利活用のロードマップ案が提示されればリアリティが上がり、ユースケースも実践的になっていくものと考える。、また、政策との連携についても具体的なロードマップが示されていない

（２） 示唆と提言

Trusted Web が国内でのみしか使えないとすれば、グローバル・サプライチェーンが常態化した現状では、普及は難しいと考える。

したがって、各国、各業界で Trusted Web の考えに基づいた相互接続や標準化について、実証や連携活動を通じて進めるべき段階にある。

以下図 5.2.2-1 にグローバル連携、業界横断の連携スキームの案を示す。

今日のサプライチェーンは、業界ごとに異なる仕組みでトラストを確保する仕組みを検討している。たとえば、IT 業界、OT(Operation Tecknology)業界、半導体業界、ソフトウェア業界などはそれぞれ独自のトラスト検証技術をもっている。

しかしながら、これらの業界間をまたがって部品や製品が提供されており、トラストの伝搬は個別あるいは十分には実施されていないのが現状である。
また、サプライチェーンはもはや一国にとどまらず、グローバルに広がっているのが当たり前であり、各国のサプライチェーンもつながっている。
このため、業種間、各国間のサプライチェーン上で、オープンな仕組みで安全にトラストをつないでいく、いわゆる「Trust Chain」が必要である。
このためには、TN のようなプロトタイプを用いた国際接続検証や国際標準化といった活動により、トラストのサイロ化を避けていくことが、Trusted Web に求められると考える。

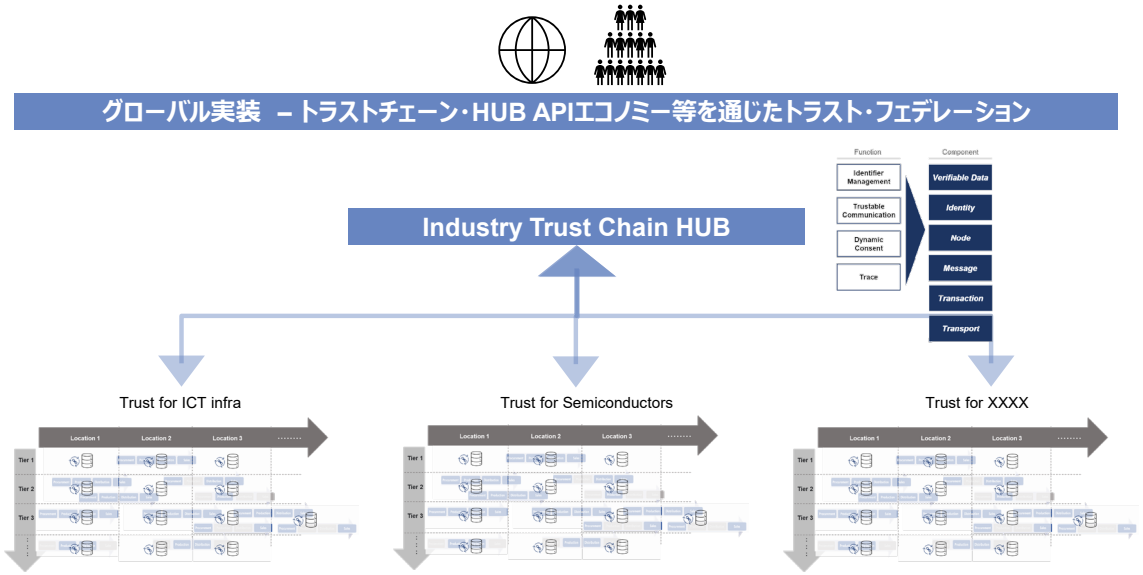


図 5.2.2-1 グローバル・異業種間のサプライチェーン・トラストのチェーニング

付録 A. TNP が管理する情報とその属性