令和3年度補正予算Trusted Web共同開発支援事業費
「Trusted Webの実現に向けたユースケース実証事業」
最終報告書概要版

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

アラクサラネットワークス株式会社

2023年3月24日

目次

01

背景・目的

1.1 背景

信頼性・安全性の確保とコストの最適化

- **ITインフラ機器のサプライチェーンセキュリティ向上が社会課題**
  具体的な対策として、機器調達時の**真正性**（不正改ざん無し）、運用中の**真正性・脆弱性確認**が強く求められる
- 各事業者（機器利用者）による真正性確認情報収集は、ベンダ・インテグレータの個別対応も要し、**多大なコストが発生**、日本全体で大きな経済的コストとなる
- 一方、経済安全保障の観点からも、サプライチェーンセキュリティ確保・向上は必須であるが、各種法制に対して事業者の負担にも配慮すべきとの意見が出ている
- 社会全体として共通的に取り組むべき課題であるが、事業者、インテグレータ、ベンダがIT機器とその機密情報を主体的に取引し、コントロール、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、が実現上の絶対的な要件であり、これは**Trusted Webのコンセプトと合致**する
- 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、コストの分割損やバラつき、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

1.1 背景

業界全体として求められる対応

●日本の重要インフラへのサイバー攻撃が激化。特に、**サプライチェーンを標的とした攻撃のリスクが増大**

●サプライチェーン攻撃の手口
- ✓ 安全性（信用度）の低い部品を利用したIT機器を狙う
- ✓ サプライチェーン上での不正な改ざんによるバックドアの仕込み
- ✓ ソフトウェア/ハードウェアの脆弱性を突く、など

●このため、**経済安全保障推進法**(‘22/5成立)にて、基幹インフラの安全確保に向け、14の基幹インフラ業種で導入する重要設備（IT機器含む）の事前審査を受けることが事業者に義務付けられた

●しかしながら、IT機器の安全性を担保するための信頼できる情報をサプライチェーン全体に渡って、どのように確認・検証するのか、**技術と業界全体での取組み体制が確立していない**

→ 日本として国家的取り組みが求められる社会課題

信頼に足る、IT機器の構成情報、素性情報を流通させる仕組みとして**Trusted Networkエコシステム**を立上げ、共創により日本のITインフラのトラスト向上を実現する

1.2 目的

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機器の調達・運用する際に、

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

④ 当該製品と当該信頼情報の**真正性**（唯一無二かつ不正改ざんされていないこと）の検証

⑤ 当該製品の**永続的な信頼性（信用情報）の検証**

を提供することにより、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。

これはTrusted Webのめざすデータのコントロールや合意形成、トレース可能化、検証可能領域の拡大と共通であり、Trusted Webのユースケースとして実証評価を進めることとした。

02

実証の概要

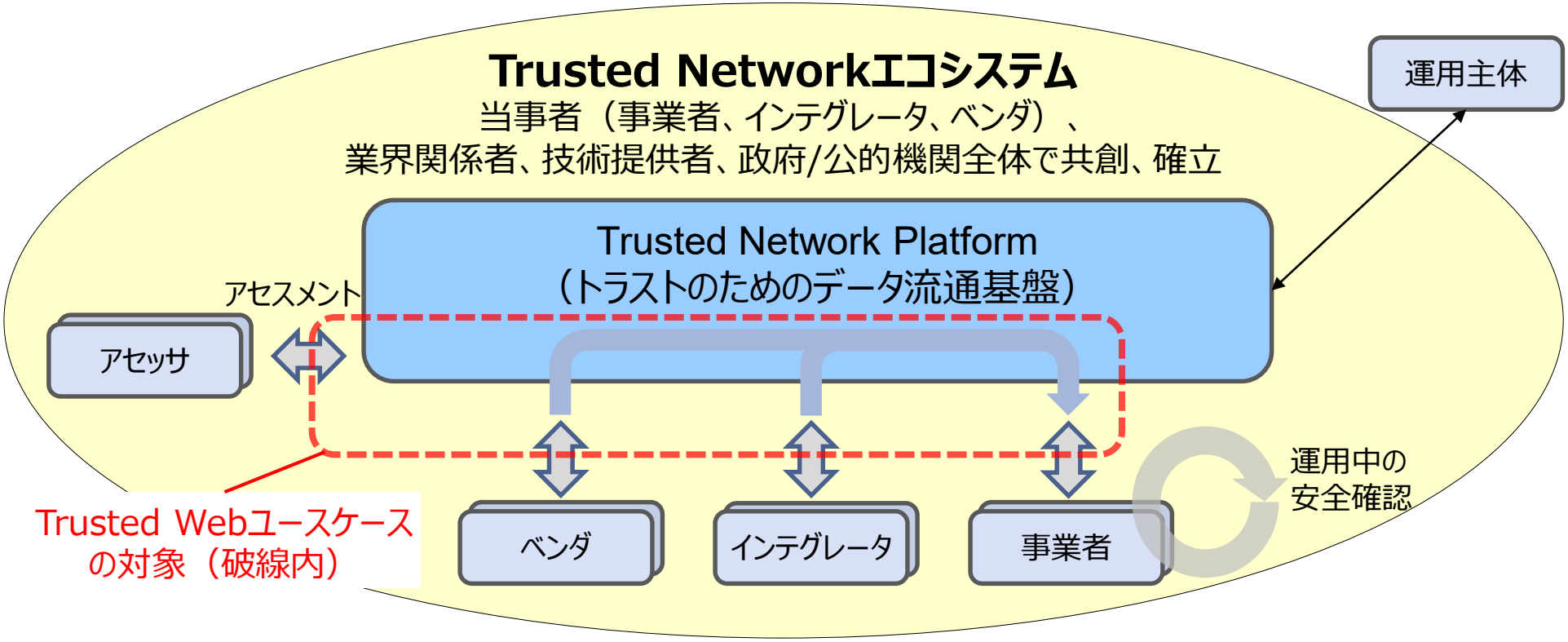
2.1 実証概要及び実証の範囲

Trusted Networkは、IT機器の調達と、導入後の運用において、真正性や脆弱性の状況を常に確認可能とした、Trusted Webの基本要件を満たすオープンプラットフォーム。

Trusted Networkの実現に向けて、以下の取組を進めてきた。

(1) IT機器調達、運用におけるトラスト要件を充足する仕組みの構築

(2) エコシステムによるオープンな共創



2.1 実証概要及び実証の範囲

Trusted Networkで実現したいこと

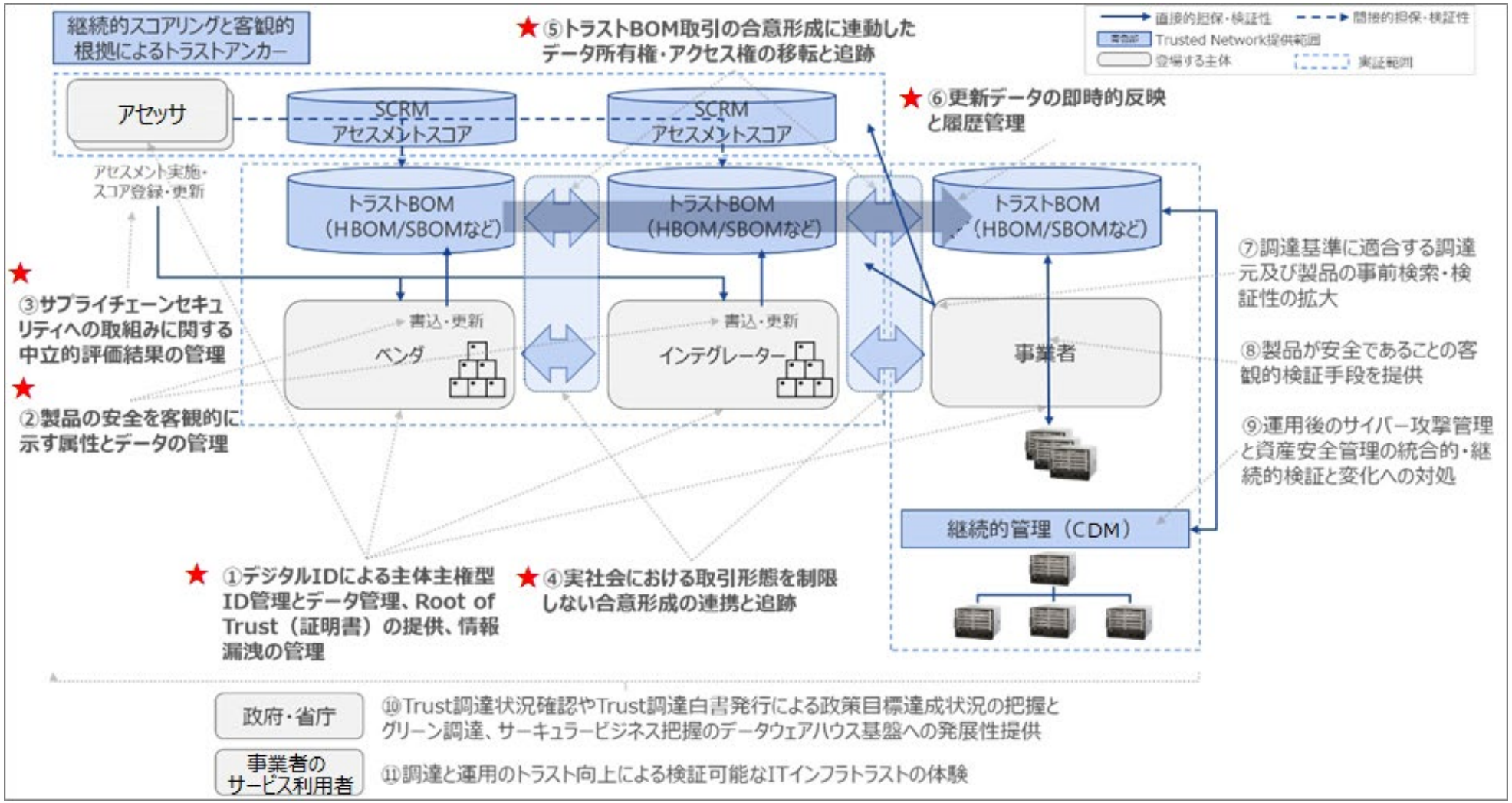
- ITインフラ調達者（事業者）が必要とする製品信頼情報（Trusted Networkではトラストbomと呼ぶ）を提供し、事業者はトラストBOMを利用することでITインフラ運用における継続的な信頼性（安全性）の検証を実施可能とする

- トラストBOMは、製品のハードウェアやソフトウェアの構成などベンダの企業機密にあたる機微な情報も含むため、この情報が改ざん又は漏洩されること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の提供により情報の信頼性連鎖も実現する

- 従来の個別対応による製品信頼情報の授受に係る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、Trusted Network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する

2.1 実証概要及び実証の範囲

本事業では、Trusted Networkにおいて以下の①～⑥のユースケース(★印)の実証を行った



BOM: Bill of Materials, SBOM: Software BOM, SCRM: Supply Chain Risk Management, CDM: Continuous Diagnostics and Mitigation

実証概要及び実証の範囲

実証で登場する主体の定義と役割

主体（組織・個人）	設定・役割	関連TWユースケース
アセッサ	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(*1)への適合状況・度合いをアセスメント、ベンダの製品のセキュリティ基準(*1)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TN上で開示することで、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。アセッサは、ベンダやその製品、インテグレータが信頼に値するかどうか、そのレベルのお墨付きを与える役割をもつ。そのためアセッサは、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。 (*1) 米国NISTの発行するSP800-161やISO27001 (ISMS)など。	①、③、⑥
ベンダ	事業者の設備を構成する機器、ソフトウェアを開発し、インテグレータを介して事業者に提供する供給元。ベンダの機器、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、ベンダが自社で開発、あるいは部品ベンダ・ソフトウェアベンダから導入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。提供する製品のTBOM（HBOM、SBOMや設定情報、付加情報など　）を登録し、トラスト保守サービス　（事業者に対して、TBOMを提供、更新をサポートするとともに、TBOM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）をインテグレータあるいは事業者に直接提供する。 アセッサによるアセスメントを受けることで自社の製品やデータのトラストを高めることができる。	①、②、④、⑤、⑥
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事業者に導入し、事業者のシステム構成に基づいて設定を行う。また、必要に応じ機器やソフトウェアの更新を含む保守を行う　。事業者に納入するITシステム　のTBOM（インテグレーションやキッティング、設定情報、更新したソフトウェアのVer.番号など）を登録し、ベンダのトラスト保守サービスを包含したシステムトラスト保守サービスを提供する。アセッサによるアセスメントを受けることで自社のトラストを高めることができる。	①、②、④、⑤、⑥
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）。事業者がサービス提供に必要となる設備（IT機器を含む）の導入・構築にあたっては、通常、システムインテグレーション事業者（インテグレータ）に委託して行う。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。 調達における主体要件を定め、TNシステムを利用し主体要件の実効性検証や調達可能なインテグレータやベンダの検証を実施する。　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。	①、②、④、⑤、⑥
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。 たとえば、省庁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サービスシステムに適用されているIT機器のトラストを、ATM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）	－

2.1 実証概要及び実証の範囲

本事業で実証する対象は以下の①～⑥のユースケース（シナリオ）である。⑦～⑪については今回の実証事業の対象ではないが、自社のプロジェクトとして実証を実施あるいは検討中である。

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の提供、情報漏洩の管理

②製品の安全を客観的に示す属性とデータの管理

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

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

⑤トラストBOM取引の合意形成に連動したデータ所有権の移転と追跡

⑥更新データの即時的反映と履歴管理

⑦調達基準に適合する調達元及び製品の事前検索・検証性の拡大

⑧調達した製品が安全であることの客観的検証手段を提供

⑨運用後のサイバー攻撃管理と資産安全管理の統合的・継続的検証と変化への対処

⑩Trust調達状況確認やTrust調達白書発行による政策目標達成状況の把握とグリーン調達、サーキュラービジネス把握のデータウェアハウス基盤への発展性提供

⑪調達と運用のトラスト向上による検証可能なITインフラトラストの体験

2.1 実証概要及び実証の範囲

Trusted Webの各要件に係る実証内容は以下のとおり

(1)Trusted NetworkによるDID発行

Trusted Network利用契約に連動しDIDを発行

Trusted Networkシステムでは、主体者の登録に際してW3Cに準拠したDIDを発行する

(2)製品やシステムの信頼性が検証可能な属性情報による動的な合意形成

ITインフラの調達に際し、事業者はトラストアンカー情報や製品信頼情報の属性情報を事前検証し、動的に合意形成を可能とする

Trusted Networkシステムは、主体者の合意形成に応じてデータ利用権及びアクセス権を移転

(3)装置信頼情報の利用権移転及び参照履歴を関係主体者が閲覧できる

自社が提供した装置信頼情報の漏洩や不正利用を防止するため、各主体がコントロールするデータの利用権の移転やアクセス状況をトレースし、必要に応じて利用を遮断可能とする

Trusted Networkシステムでは、合意形成履歴とデータアクセス履歴を記録

(4)装置信頼情報の更新が利用権保有者に伝達反映される

ベンダやインテグレータが装置信頼情報を更新した際、そのデータの利用権を有する事業者に変更と変更内容が伝達されるため、保有資産の脆弱性やリスクをリアルタイムに検証可能とする

2.2 社会・経済に与える価値・影響

Trusted Networkが解決をめざす課題

- ハードウェアとその部品（半導体等）の開発・生産の国際分業化、オープンソースソフトウェアの活用やソフトウェア開発の請負化などにより、サプライチェーン管理の重要性が高まっている
- しかしながら、サプライチェーンでの製品構成情報（正規品かどうか、不正改ざんがされていないか、脆弱性が存在していないか等）を業界横断で必要最低レベルの情報提供/取得を可能とする仕組みが存在しないためサイロ化が進行
- 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が確立されておらず、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ソフトウェアからサプライチェーン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、革新的かつ網羅的な対策が遅れている。
- 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 社会・経済に与える価値・影響

■ ユースケースが解決し得る課題と効果

#	ユースケース	効果（価値・影響）
①	デジタルID(DID)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	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	製品信頼情報（トラストBOM）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 社会・経済に与える価値・影響

■ Trusted Networkエコシステム参画者ごとの価値・影響

プレーヤー	提供価値・影響
事業者 （重要インフラ事業者）	・経済安全保障推進法で求められる製品の情報、運用委託先のセキュリティ情報が一括して入手可 ・マルチベンダ、マルチインテグレータ環境において、均質な製品安全情報を把握 ・調達製品の真正性確認、運用中の改ざん検出を容易に実施可 ・セキュリティ情報を一元管理することで、安全性が向上
インテグレータ	・アセスメントによる安全性の客観的評価を向上 ・製品、設定・運用における真正性、脆弱性等のセキュリティ情報を把握するコスト・時間を短縮、一様化
ベンダ	・インテグレータや事業者からの情報提供要求に対し、個別に対応する必要がなくなる/減る ・アセスメントを受けることで、自社の製品やデータのトラストを高めることができる。 ・デジタル情報をトラスト保守サービスとして提供できる。
政府機関	・経済安全保障推進法の実効性を高めることができる ・事業者の調達状況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うとともに、トラストBOMを活用した調達事前審査の検証性強化と検証性範囲拡大によりトラストガバナンスを堅持できる
TNE ※ (Trusted Network Enabler)	・自社だけでは提供できない総合的な価値の提供に加われる ・自社のサービス提供にあたり、個別の契約交渉や決済手段の準備が不要 ・オープンイノベーションを通じて、新たなアイデアや技術を獲得・提案し、エコシステムのサービスを拡張することで、収益を高めることができる。

※ TNP（TN Platform）にシステムの機能や技術（ライセンスを含む）や運用支援を提供

2.2 社会・経済に与える価値・影響

■ Trusted Networkエコシステムが提供する将来価値

より多元的なトレーサビリティへの拡張が可能

- デジタルIDに紐づけて様々な情報をあらかじめ記録しておけば、求めらた時すぐに提示できる。例えば、
  - 素材・部品に化学的に不適切な有害物質が含まれていないこと
  - 人道上問題となる労働力を使用していないことなどの第三者による証明
  - あるいは、製造過程における二酸化炭素排出量やエネルギー消費量の数値、など、多岐に渡る

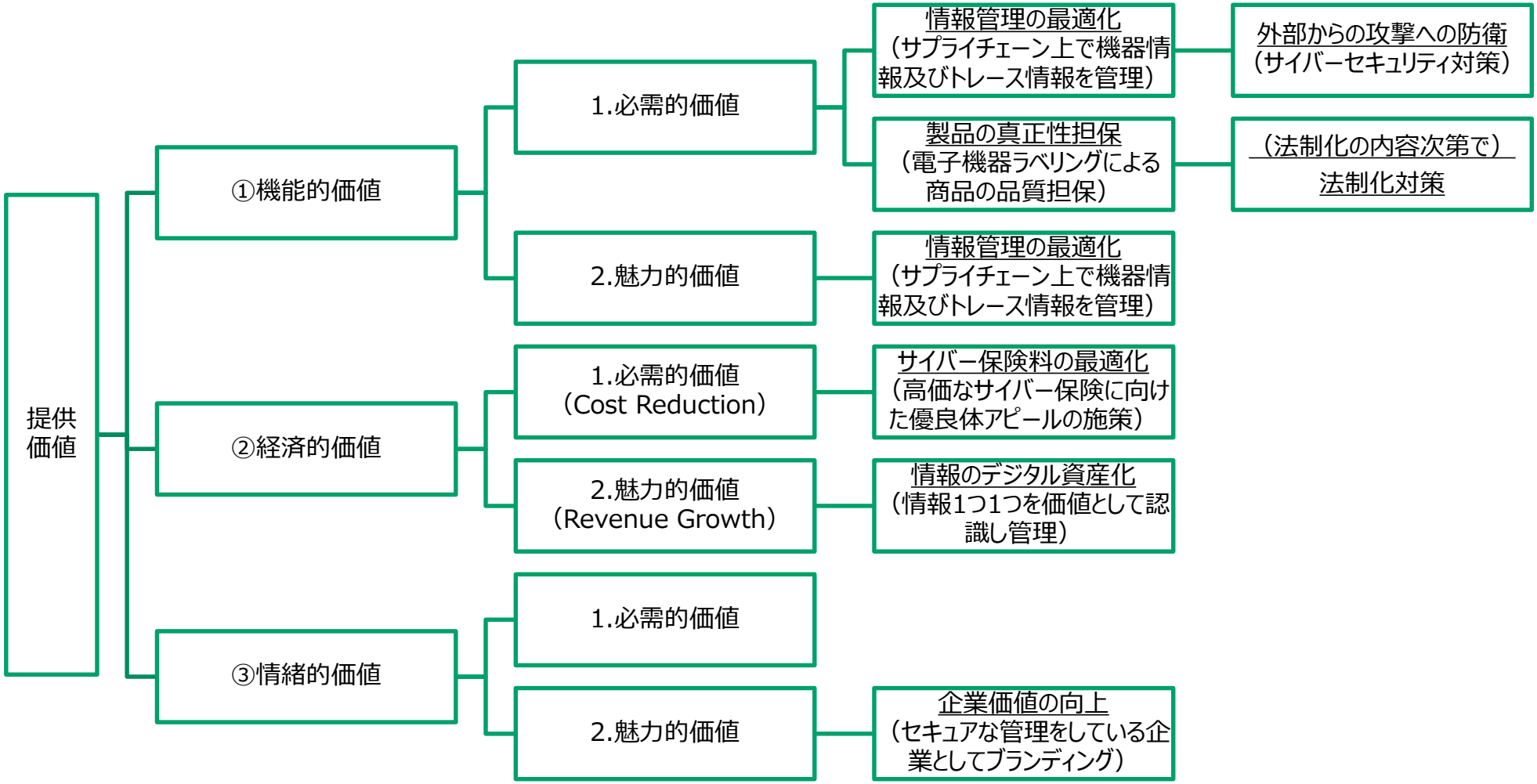
- 人権デューデリジェンス（人権DD）に対応した情報把握
  - 企業が事業活動において社内や取引先における人権侵害リスクを適切に把握し、予防もしくは軽減するための調査・分析および是正に向けた活動
  - アメリカでUFLPA（ウイグル強制労働防止法）が制定・施行され、OECD／国連により人権DDガイドラインが制定される中、国内においても、経済産業省が「サプライチェーンにおける人権尊重のためのガイドライン（案）」をまとめている。

- デジタルプロダクトパスポート
  - 欧州では製品や部品のサステナビリティ情報を提供する仕組み（導入が検討されている）
  - 循環経済実現に向け、欧州に上市される製品のサステナビリティ情報を提供するもので、適切な対応にはサプライチェーンを通じた情報収集や、社内でのシステム・体制構築が必要となる。

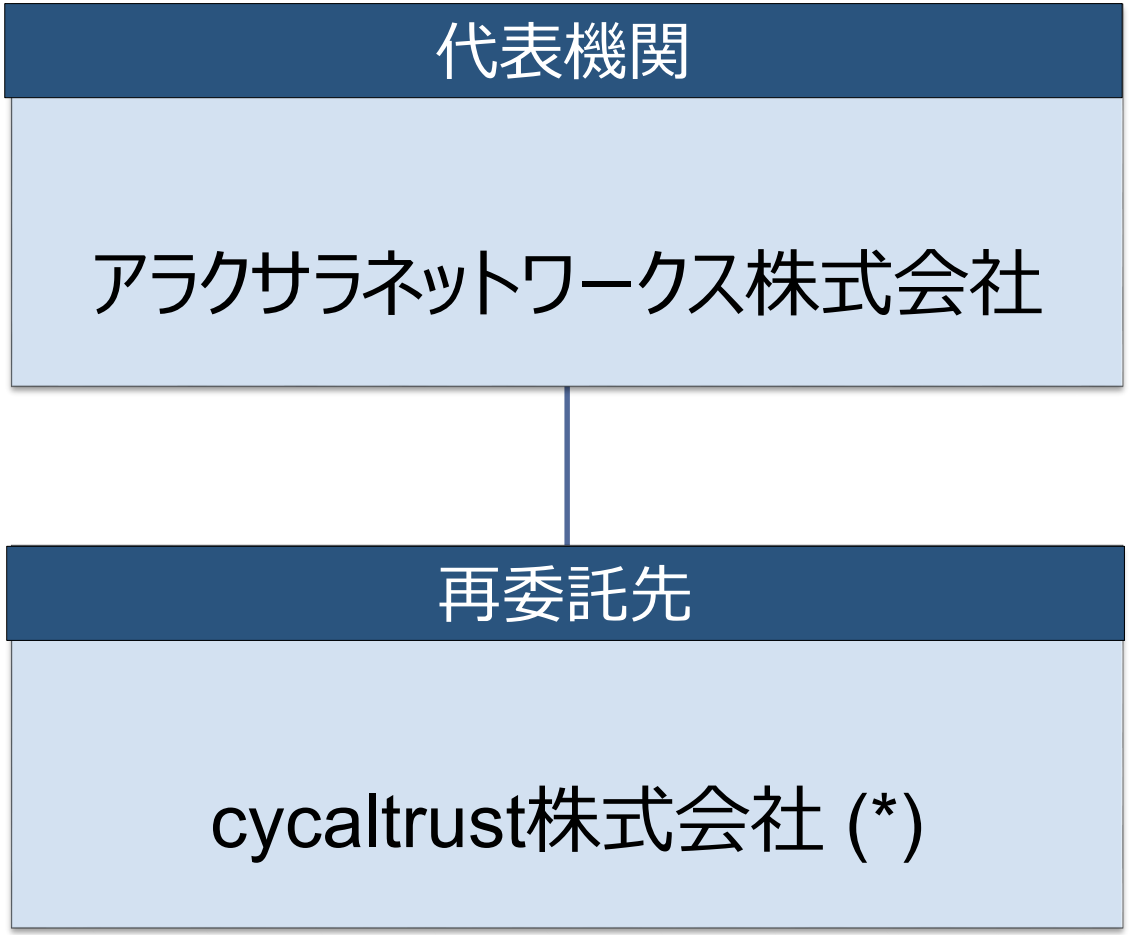
➔ 新たな情報定義、情報提供者、情報提供先に、すばやく、低コストで対応可

2.2 社会・経済に与える価値・影響

■ Trusted Networkの提供価値の全体像



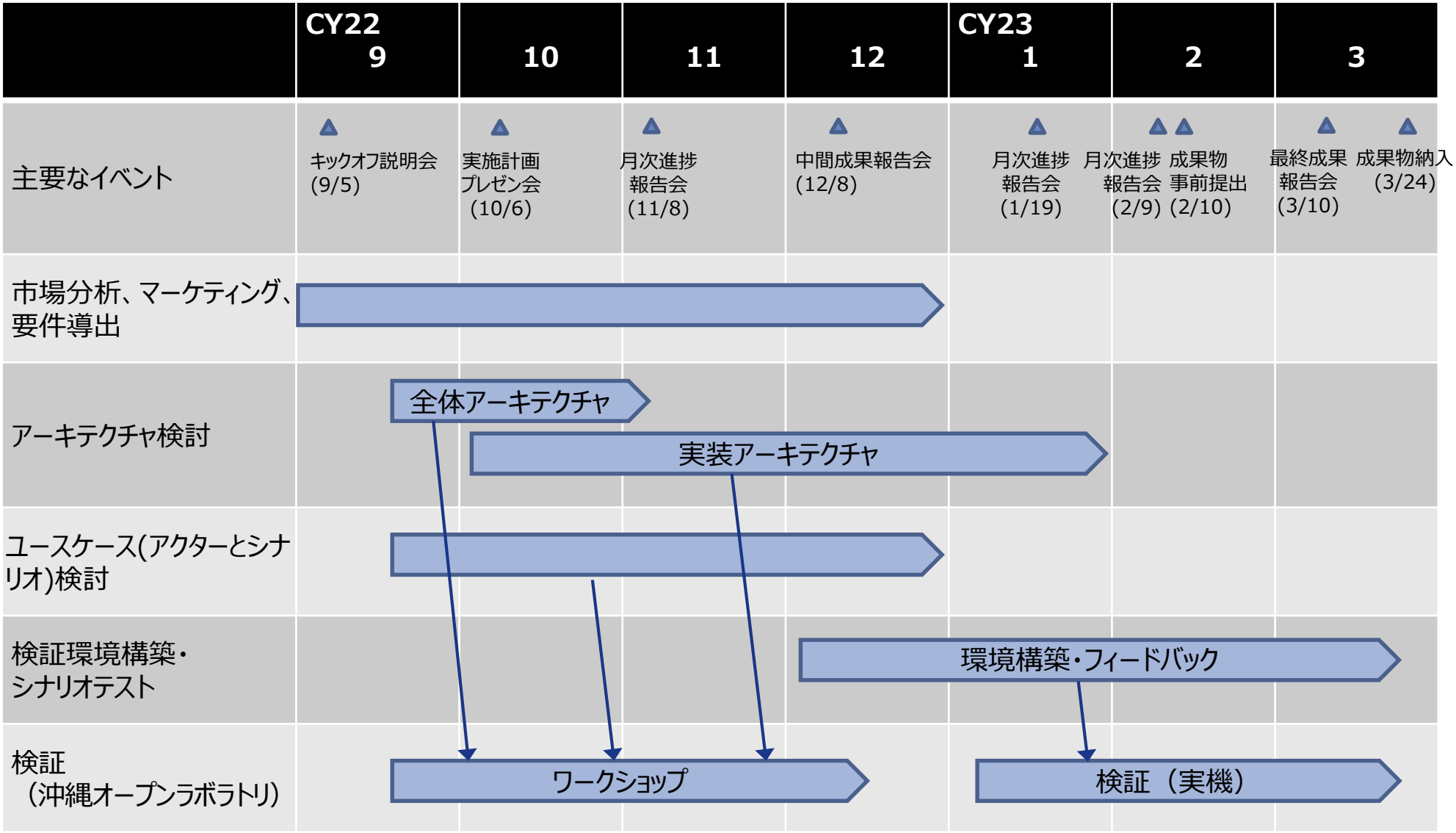
2.3 コンソーシアムの体制



ブロックチェーンを利用したデータの登録・参照コントロール、検証、トレース等の技術検討

*: cryptomall japan 株式会社から社名変更（ 2023/1/6）

2.4 実証全体のスケジュール

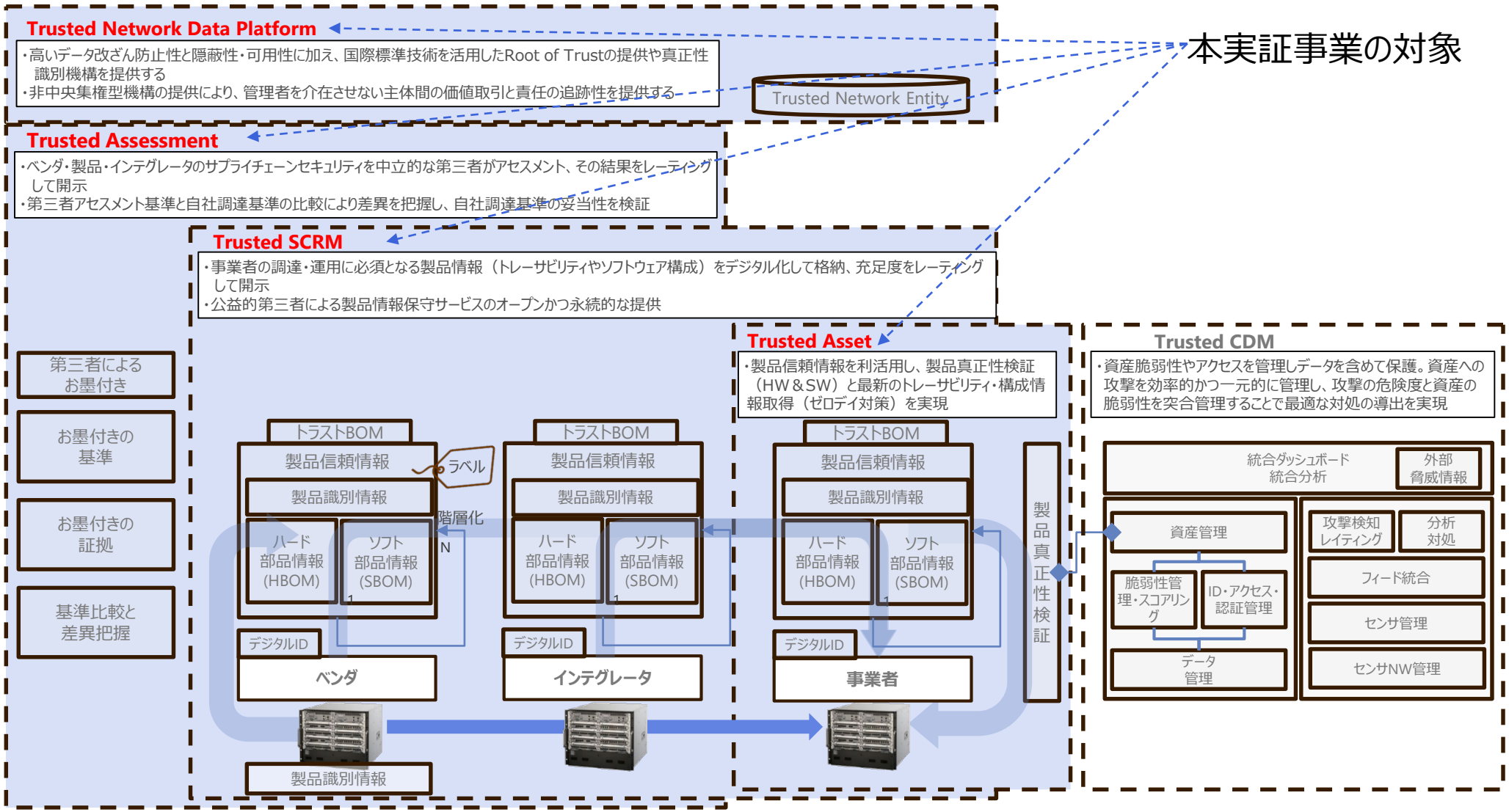


03

実証内容

3.1 実証の実施事項、論点及び判断（1/3）

Trusted Networkの構成と機能



CDM: Continuous Diagnostics and Mitigation, H/SBOM: Hardware/Software Bill of Materials, SCRM: Supply Chain Risk Management

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

■ 実証の進め方

- 本実証事業は、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）に発足したTrusted Networkプロジェクト（TN-PJ）にて検証を実施した
- TN-PJでは、本実証事業の受託範囲外の実証も自主事業として実施中

項目	内容
プロジェクト名	Trusted Network (TN)
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・SIer・事業者・利用者・政府等、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	● ワークショップフェーズ（2022/9/30～12/9） 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 ● 検証フェーズ（2022/12/23～3/E ） 実システムのデモ、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 ● 討論会（パネルディスカッション） 評価結果発表と国内外政府機関を含む関係者との意見交換を実施
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 PJメンバ：沖縄オープンラボ会員、その他一般から募集

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

■ 沖縄オープンラボ TN-PJで実施したワークショップの内容

#	ワークショップのトピックス	月日
1	Trusted Network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)

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

■ 沖縄オープンラボ TN-PJで実施したデモ・検証の内容

#	ワークショップのトピックス	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））	2022/12/23(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）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)
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 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

実施事項	論点	判断
要件定義	TNへのユーザ確認（なりすまし対策）	登録者であることを確認するためにDIDを使用
	TNへのデータ確認	データ登録者を確認するためにVCを使用
	ブロックチェーンの選定	非公開要件への適合、ノード間のネゴシエーション機能を備えているため「Quorum」を選定
基本設計	製品の真正性確認方法	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）
	Dynamic Consentの記録場所	ブロックチェーンに記録する
	ベンダ、インテグレータ、その他、事業者への製品の流れ	ブロックチェーンでNFTを移転させることで実現
	トラストBOMの保存場所	分散型ストレージにて管理を行う
	SBOMのフォーマット	標準化されたフォーマットとして、もっとも広く普及している「SPDX」を採用
システム開発	トラストBOMの作成フロー	ベンダーから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
	トラストBOMの開示請求フロー（個によるデータコントロール）	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
	トラストBOMへの記録方法と記録内容（検証可能な領域の拡大）	検証可能領域の拡大として、TBOM情報をIPFS等に置いた。ブロックチェーン+IPFSでデータ量が増えた。 IPFSとブロックチェーンを組み合わせることで、データサイズの大きいものも対応できるようになった。Traceの内容が増えた。TBOMのトレース TBOMの更新情報・BOMの内訳を残す 重大なインシデントが発生したときに、お客さま自身で判断することができる。

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

■ 本実証事業で検討・検証したTrusted Networkの基本機能（要件）は以下のとおり

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（TBOM）は、ハードウェア信頼情報（HBOM)、ソフトウェア信頼情報（SBOM)のがある。 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明らかにしているか（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。

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

■ 本実証事業で検討・検証したTrusted Networkの基本機能（要件）は以下のとおり

機能要素	概要
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。 ・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）

3.1 実証の実施事項、論点及び判断（1/3）

プロトタイプシステムの企画・開発

プロトタイプに実装した機能

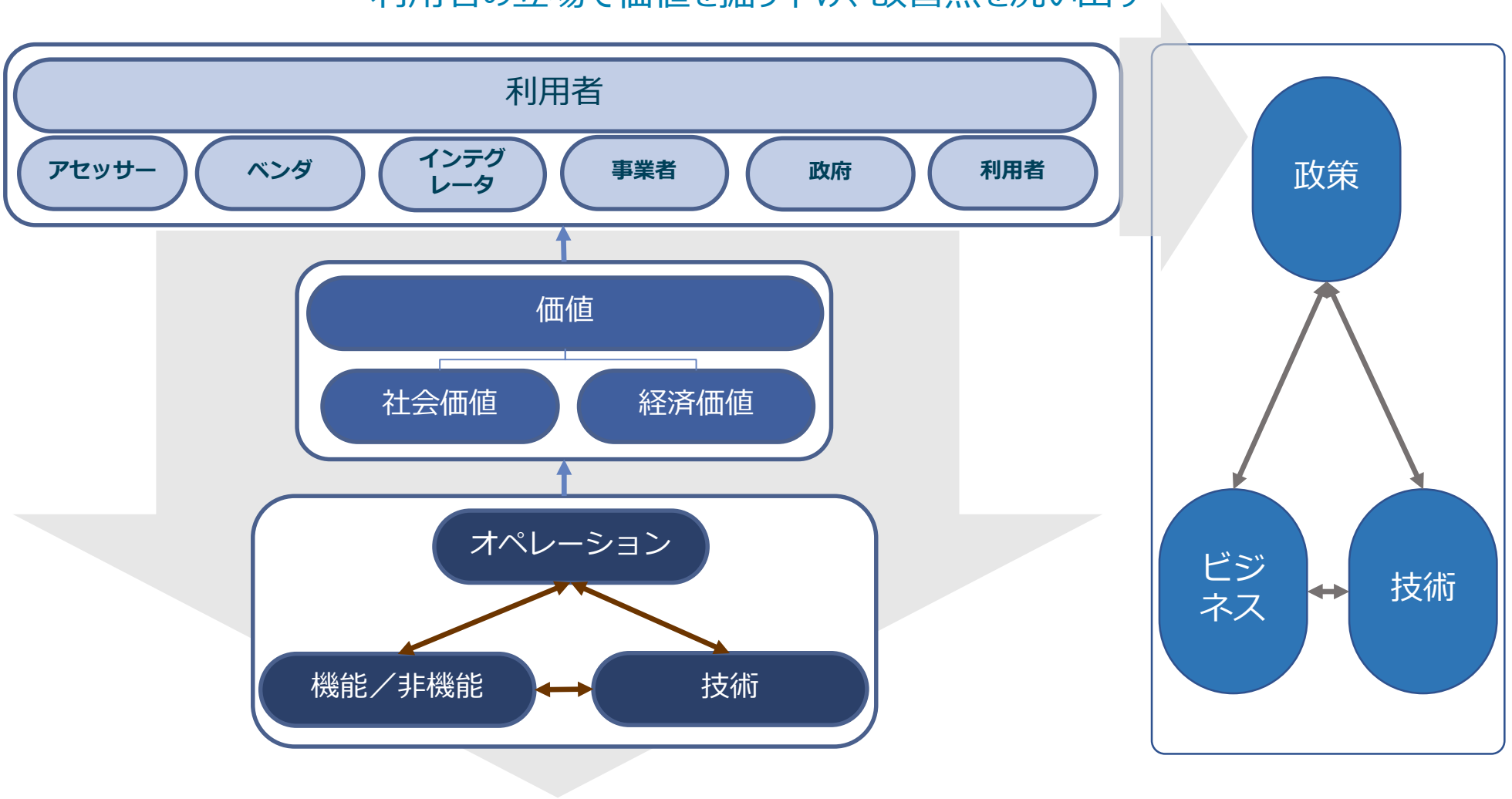
基本機能	個別機能	内容
Trusted Assessment	トラストレーティング	ベンダ・製品・インテグレータのサプライチェーンセキュリティレベルを中立的な第三者がアセスメント、その結果をレーティングして一元的に開示
	トラストマッチング	第三者によるアセスメント基準と自社調達基準の突合比較により差異を把握し、製品やインテグレータの自社調達基準への適合性を検証
	トラストアンカー	ベンダ・製品・インテグレータのアセスメントをデジタル資産化し、証明書／エビデンスを付帯して提供
	アセスメント as a service	事業者様の調達主体要件や政府調達基準を基準にした継続的アセスメントサービスの提供
	ビジネスマッチング	ベンダ・インテグレータのアセスメント対応労力を最小化と、その成果への経済的価値の付帯
	Root of Trustとトレーサビリティ	アセスメント関連データへのVC付帯（DID/SSI技術）によるRoot of Trustの確保とアセスメントトレーサビリティの提供（ブロックチェーン技術）
Trusted SCRM	デジタルパスポート、情報充足度レーティング	事業者の調達・運用に必須となる製品トラスト情報（HWトレーサビリティやSW構成）をデジタル資産化しトラストパスポートを提供するとともに、情報の充足度をレーティングしてダッシュボード表示
	トラスト保守	公益的第三者（政府クラウド基盤等の活用含む）を介したトラスト保守サービス（トラスト情報・トラストパスポート・信頼証明書提供サービス）の永続的提供を実現
	コスト最適化	ベンダやインテグレータに対して統一的かつ共通的な手順と自動化を提供することで事業者へのコスト負担を最小化するとともに、細やかなカスタマイズへの対応を両立
	検証	調達資産の透明性や調達主体基準への適合性に関する検証性を提供、政府機関への証明書付き情報提供に対応
	Root of Trustとトレーサビリティ	トラストデータへのVC付帯（DID/SSI技術）によるRoot of Trustの確保とトラストデータトレーサビリティの提供（ブロックチェーン技術）

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリングの論点

沖縄オープンラボのTrusted Network PJのPOV(Proof of Value)にて、以下の視点で検証結果を取得・整理する（’23/3）

利用者の立場で価値を掘り下げ、改善点を洗い出す



3.1 実証の実施事項、論点及び判断（2/3）

ヒアリングの論点

■ 検証事項一覧（沖縄オープンラボのPOVにて評価中）

検証観点1	検証観点2	検証観点3	検証スコープ	検証内容
PJの目的・ゴール	課題設定	課題の確からしさ（正確性）	システム全体・マクロ評価	● 本PJで定義した課題が現実社会の課題を正確に捉えているか
				● 課題設定への示唆や提言
		あるべき姿の適切性		● 本PJで定義したあるべき姿が現実社会の目指すべき世界を適切に示しているか
				● あるべき姿に関する示唆や提言
	価値の有無	社会的価値		● 本PJの目的やゴールについて、社会的価値の有無や価値発生の条件を検証する
				➢ 課題設定に根本的かつ致命的な問題があるので評価不能
				➢ 価値が不十分であり改善の余地は無い（理由を併記）
				➢ 価値が不十分であるが改善すれば十分となり得る（条件の有無や改善への示唆や提言を併記）
				➢ 価値は十分である（条件の有無や改善への示唆や提言を併記）
				● 社会的価値を高めるための示唆や提言
		経済的価値		● 本PJの目的やゴールについて、経済的価値があるかを検証する。
				➢ 価値に対して価格が高いが使う（理由や条件を付記）
				➢ 価値に対して価格が高いので使わない（適切なコスト感の示唆や提言を付記）
				➢ 価値に対して価格が適切だが使わない（理由と解決策（どうしたら使うか）に関する示唆や提言）
				➢ 価値に対して価格が適切なので使いたい（理由や条件を付記）
				● 経済的価値を高めるための示唆や提言
価値実現手段	機能	機能／非機能適切性	サブシステム個別・ミクロ評価及びシステム全体（E2E）視点	● 価値を提供するための機能設計（仕組み）は妥当か
				● 非機能要件（機密性、信頼性、拡張性など）に関する設計（仕組み）は妥当か
				● 適切な代替機能など、改善に関する示唆や提言
		機能拡充性		● 価値を提供するための機能性や網羅性は十分か
				● 不十分な部分についての指摘、改善に関する示唆や提言
	技術	技術／製品適切性		● 価値を提供するための機能（仕組み）に適用されている技術や製品は適切か
				● オープン性、相互接続性、秘術信頼性、将来も含めた安定性、使用性などの非機能要件に懸念は無いか
				● 不適切な部分についての指摘、改善に関する示唆や提言
価値提供オペレーション	操作性	操作適切性		● 価値を提供するための操作やオペレーションの設計は適切か
				● 使用性、効果性、効率性、保守性、習熟性などを含めた保守運用性全般
				● 不適切な部分についての指摘、改善に関する示唆や提言

3.1 実証の実施事項、論点及び判断（2/3）

ヒアリングの論点

■ 検証事項一覧（沖縄オープンラボのPOVで得られた評価）

検証観点2	検証観点3	検証内容
課題設定	課題の確からしさ（正確性）	● 本PJで定義した課題が現実社会の課題を正確に捉えているか
		● 課題設定への示唆や提言
	あるべき姿の適切性	● 本PJで定義したあるべき姿が現実社会の目指すべき世界を適切に示しているか
		● あるべき姿に関する示唆や提言
価値の有無	社会的価値	● 本PJの目的やゴールについて、社会的価値の有無や価値発生の条件を検証する
		➢ 課題設定に根本的かつ致命的な問題があるので評価不能
		➢ 価値が不十分であり改善の余地は無い（理由を併記）
		➢ 価値が不十分であるが改善すれば十分となり得る（条件の有無や改善への示唆や提言を併記）
		➢ 価値は十分である（条件の有無や改善への示唆や提言を併記）
		● 社会的価値を高めるための示唆や提言
	経済的価値	● 本PJの目的やゴールについて、経済的価値があるかを検証する。
		➢ 価値に対して価格が高いが使う（理由や条件を付記）
		➢ 価値に対して価格が高いので使わない（適切なコスト感の示唆や提言を付記）
		➢ 価値に対して価格が適切だが使わない（理由と解決策（どうしたら使うか）に関する示唆や提言）
		➢ 価値に対して価格が適切なので使いたい（理由や条件を付記）
		● 経済的価値を高めるための示唆や提言

主な意見・コメント

- ✓ 課題設定は概ね十分
- ✓ 類似活動との連携が必要
- ✓ 国際動向の把握が必要
- ✓ スピード感が重要（国際競争）
- ✓ 中立的第三者の明確化

- ✓ 不十分だが改善に寄り対処可能
- ✓ エコシステム拡大が課題
- ✓ 想定価格が高い（価値の納得性が不十分）
- ✓ 経済安全保障とは距離がある
- ✓ 真正性検証機器の価格に依存

3.1 実証の実施事項、論点及び判断（2/3）

有識者へのヒアリング

ヒアリングの目的	対象	ヒアリング結果
Trusted Networkの実現に必要な事項を把握するため	セキュリティビジネスの専門家	セキュリティの世界観からの視座の提供 • セキュリティの世界は実際に何かが起こらないと（被害が発生しないと）ビジネスが盛り上がらない • **海外への展開を視野に入れる**ことがブレークスルー要因 • **SBOMの真正性確保はキーファクター** • **米国のキーパーソンとの面談・連携** • **米国のお墨付きが有効** → **米国政府機関であるCISAの**ディレクターである**Allan Friedman氏と連携**（同氏は**SBOMが専門**） • 数社がTrusted NetworkのPoV（価値実証）に強い興味あり → レバレッジしたい
	セキュリティ機器企業	• Trusted Networkを導入した際の**ビジネスモデルの絵姿を鮮明に** • DXは技術だけではなく**視点・発想の転換も重要** • **失敗を前提とする取り組みへの発想の転換**も推奨 • 政府機関がTrusted Networkのような仕組みの実現を推進するポテンシャルは高い（**ここでもビジネスモデルの絵姿は重要**） • ブロックチェーン技術の活用での「副産物」として導入事業者にメリットを創り出せないか • 事業者・ベンダ・Sierの中で最もメリットを享受するのは事業者 ⇒ **事業者のインセンティブは何か・社内手続きが通りやすい形にするには？** • 事業者の中で「誰？」 ⇒ 購買 ⇒ **購買にとって都合の良い売り方とは？** • 政府機関と連携して「**Proven in Japan（認証のようなもの）**」を活用できないか

3.1 実証の実施事項、論点及び判断（3/3）

国際標準規格の調査

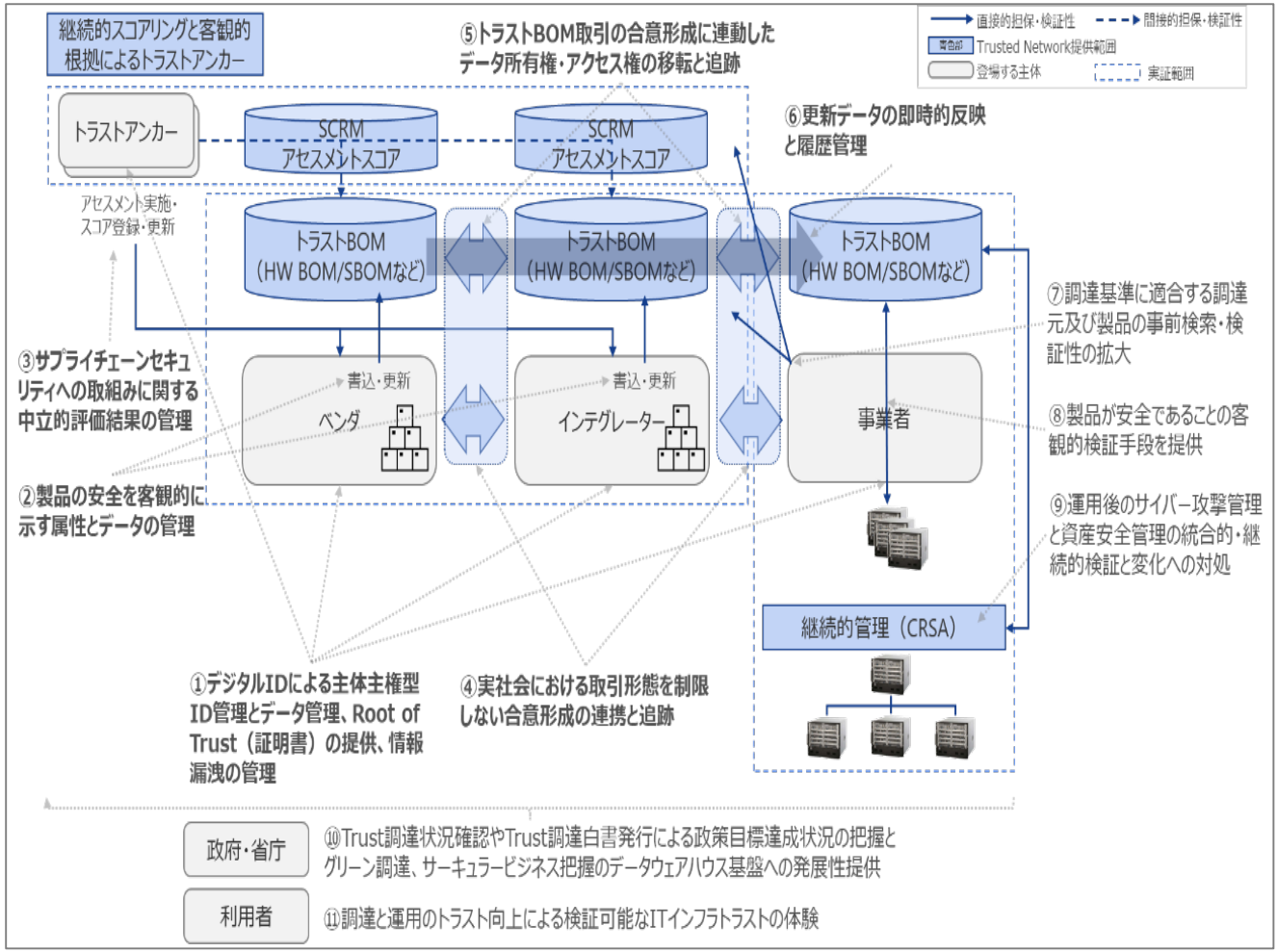
■ Trusted Networkに関する国際標準規格
関連する主な国際標準規格を示す。詳細は付録参照。

調査事項	調査対象機関	調査結果
Web 3.0	W3C他	Web3.0の概念はあるものの、詳細な定義や標準は定まっていない状態。 Trusted Networkでは、自律分散組織（DAO）、非中央集権的なWeb3.0の特徴をもちながら、運用は完全な自律分散ではなく、運用主体を公益的な第3者に委ねる前提としている。事業者の調達行為との乖離（システムとは契約できない）があるためである。
参加主体とその製品が、調達側の事業者のセキュリティ要件との適合度合い、さらには主体の信用度を評価する規準	NIST	組織とサプライチェーンも含めた包括的なセキュリティ規準としては、米国のNIST SP800シリーズが充実しており、その基準の中から、適切な規準はどれがよいのかを調査した。 Trusted Networkでは、調達から販売・供給までの一連のサプライチェーンに存在する業務委託先や関連企業のすべてにおいて、一貫したセキュリティ基準を定めたSP800-161を採用した。
製品信頼情報（トラストBOM）のフォーマット	Linux Foundation / OWASP Foundation	SPDX: Linux Foundationがオープンソースのライセンスコンプライアンスに関連する情報を扱う目的で開発したSBOMフォーマット。ISO/IEC 5962:2021で標準化。 Cyclone-DX: OWASP Foundation が開発したセキュリティを念頭に置いたSBOMフォーマット。 Trusted Networkのプロトタイプでは、社会実装の進んでいるSPDXを採用したが、基準自体はどの基準であっても適用可能なアーキテクチャとした。

OWASP : Open Web Application Security Project

3.2 検証できる領域を拡大する仕組み（1/3）

データスキーム図



登場する主体とその概要

主体	役割・設定
ベンダ	・インテグレータや事業者からの情報提供要求に対し、個別に対応する必要がなくなる/減る ・アセスメントを受けることで、自社の製品やデータのトラストを高めることができる。 ・デジタル情報をトラスト保守サービスとして提供できる。
インテグレータ	・アセスメントによる安全性の客観的評価を向上 ・製品、設定・運用における真正性、脆弱性等のセキュリティ情報を把握するコスト・時間を短縮、一様化
事業者	・経済安全保障推進法で求められる製品の情報、運用委託先のセキュリティ情報が一括して入手可 ・マルチベンダ、マルチインテグレータ環境において、均質な製品安全情報を把握 ・調達製品の真正性確認、運用中の改ざん検出を容易に実施可 ・セキュリティ情報を一元管理することで、安全性が向上
トラストアンカー	ベンダ・製品・インテグレータのアセスメントをデジタル資産化し、証明書／エビデンスを付帯して提供

3.2 検証できる領域を拡大する仕組み（2/3）

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

要検証な課題	検証対象	検証方法	検証者	保有者	発行者	データの置き場	アクセスコントロールの手法	成果・留意点
TNへのユーザ確認（なりすまし対策）	ユーザ情報の内容（署名したアイデンティティ）	VCの署名検証	初期登録時：公益的第三者であるTNPF運用者 登録後：TNPF	初期登録時：TN利用申請者 登録後：ユーザ	初期登録時：TNPF運用者が発行した利用契約書 登録後：TNPF	初期登録時：TNPF運用者と利用申請者のオフィスに契約書の写しを一部ずつ保管。その後、TN PF運用者はTN PFにユーザ登録（wallet作成・did生成・ユーザID生成・初期パスワード登録など）を実施する。 登録後：TNPF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実施	初期登録時：契約書は各事務所のフィジカルセキュリティによりアクセスコントロール。ユーザ登録時に生成される情報は、ブロックチェーン上及びセキュアストレージ上に保存され、TN PF運用者やユーザはアクセス情報を知ることが出来ない。アクセスはACLとdidの検証によって制御する。セキュアストレージノードへのダイレクトアクセスコントロール連携の仕組みについては検討課題である。 登録後：上記のユーザ登録時の情報と同じ。	設計中 TN PF運用者と利用申請者間の契約は外部電子契約サービスを利用する可能性もある。複数のエンティティ・ノードへのアクセスを統合的にコントロールする必要があるが、標準的な仕組みでは対応が困難なため独自実装せざるを得ない部分に課題がある。
TNへのデータ確認	製品およびトラストBOM情報の内容確認（データ自体）	VCの署名検証	TBOMを登録・更新するユーザ	TBOMを利用するユーザ	ベンダ自身がベンダ自身の手で	TNに登録したTBOM内容を保証する	上記のユーザ登録時の情報と同じ。	設計・開発中
アセスメント結果の確認	製品のアセスメント結果の内容（データ自体）	VCの署名検証	アセッサが	アセッシーとアセスメント結果閲覧者に	アセッサ自身が登録するエビデンスによって	アセスメント結果の内容を保証する	上記のユーザ登録時の情報と同じ。	設計・開発中
製品の真正性確認	製品シリアル番号、開封検知ICラベル情報、トラストBOM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）	NFT突合	製品とTBOMへのアクセス権を所有するユーザが	自分自身に	ベンダが登録したTBOMと製品情報、ベンダが添付した開封検知ICラベル情報、TNPFが発行した論理ギャランティーカード（NFT）を	TNPF上で突合する	上記のユーザ登録時の情報と同じ。	設計・開発中

3.2 検証できる領域を拡大する仕組み（3/3）

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

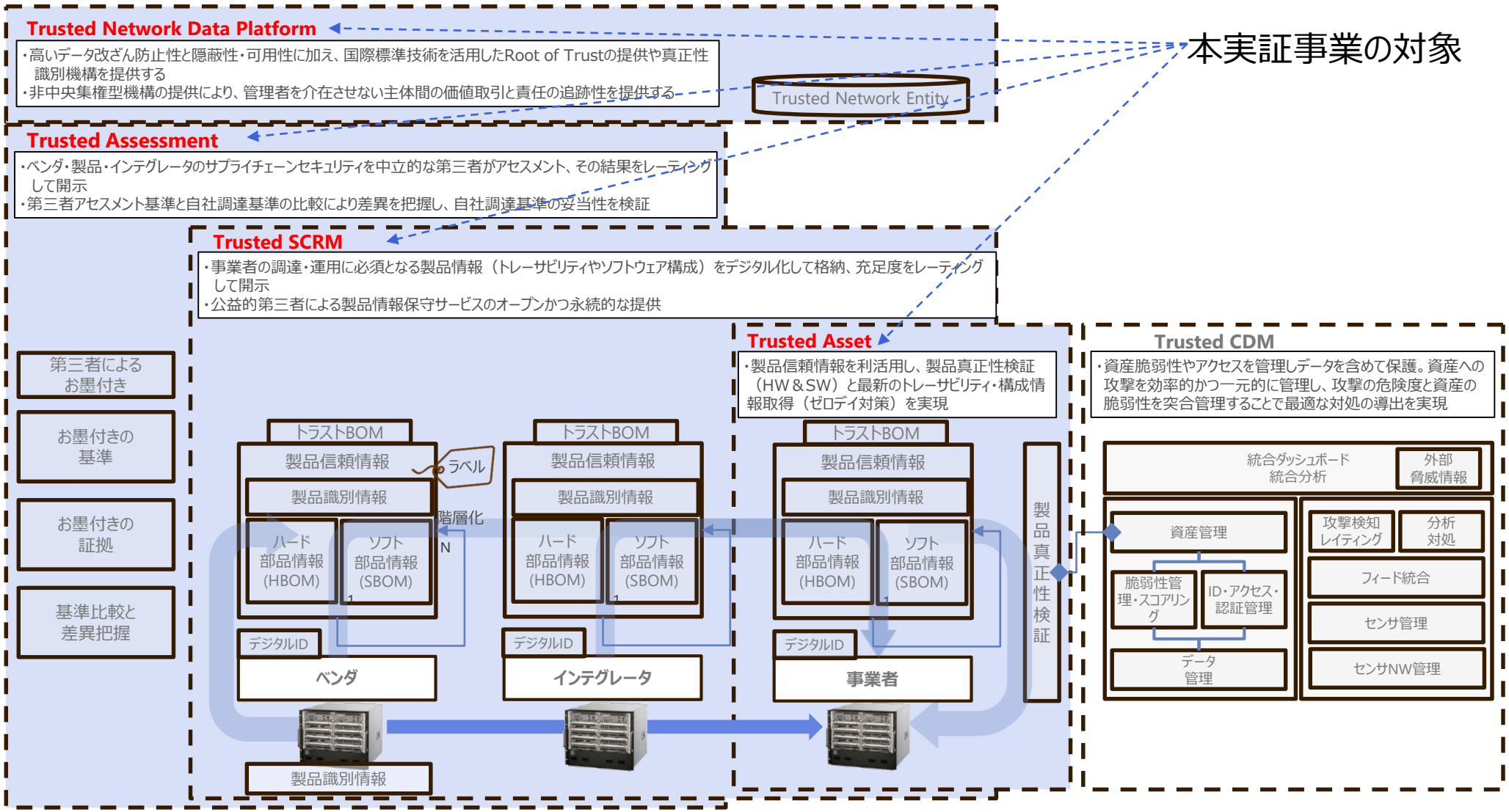
合意の主体	合意の対象	合意の条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
ベンダ / インテグレータ / 事業者/ TNDP	登録製品・サービスの一覧	Trusted Network Data Platform（TNDP）に製品・サービスを登録すること	履行された左記の合意 製品信頼情報の内容および所有権の遷移	閲覧者 (主にインテグレータ / 事業者)	・インテグレータ、事業者が、製品に不正な改ざんなどの処理が行われていないか、取引、設定履歴をトレースする ・トレースの方法としては、ブロックチェーンに以下の情報を記録し、権限をもつユーザ(DIDで識別)が履歴の確認（トレース）を行うことを可能とする - ユーザの登録情報、更新履歴 - TBOMの登録や更新の履歴とデータのパス - アセスメント保存履歴 - 製品の発送（所有権移転）	可能
	アセスメントレポート (結果)	ベンダがアセッサーに対して開示許可し、TNDPに登録すること				
	製品信頼情報（TBOM）	ベンダが製品毎のTBOMをTNDPに登録し、開示許可を設定すること				
	製品信頼情報のレーティング	ベンダが製品信頼情報（TBOM）のレーティング開示許可をTNDPに設定すること				
	真正性情報	• 主体が製品購入契約を締結 • TBOM、現品情報(シリアル、開封検知ICタグ等)の利用権であるトラスト保守を契約				
	更新した製品信頼情報					

3.3 6構成要素との対応

6構成要素		6構成要素との当てはめ
検証可能なデータ	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製品およびトラストBOM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、トラストBOM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）
	署名者	ベンダ、アセッサー（アセスメント実施者）
アイデンティティ	アイデンティティとして想定されるものが何か	ベンダ、インテグレータ、（インフラ）事業者、アセッサ
	アイデンティティ管理システム（外部）は何を利用しているか。(例：OIDC for VC, DID)	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
	アイデンティティグラフとして想定されるのはなにか	サプライチェーンにおいて、ベンダ間、ベンダーインテグレータ間、インテグレータ間、インテグレーター事業者間、ベンダー事業者間、事業者間で可視性の違いが存在する
ノード	Walletか否か	Trusted Network運営者がQuorumにアクセスするノード(エンティティ)に対して、Walletを生成する
	合意形成がされているか、されているならその手段	Quorumのdynamic consent機能を利用（ノード間通信）
	データのやりとりをどこに記録するか	ブロックチェーンに記録
メッセージ	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	メッセージオリエンテッド
トランザクション	データのやり取りを記録するか	アセスメント結果、トラストBOMの新規登録・変更、参照、所有権移転をブロックチェーンに記録
	データのやり取りの検証はできるか	エンティティがそれぞれの権限にしたがって、データのやり取りの検証が可能
トランスポート	トランスポートのプロトコルは何か	Quorum

3.4 本実証で企画・開発したシステムの概要（1/6）

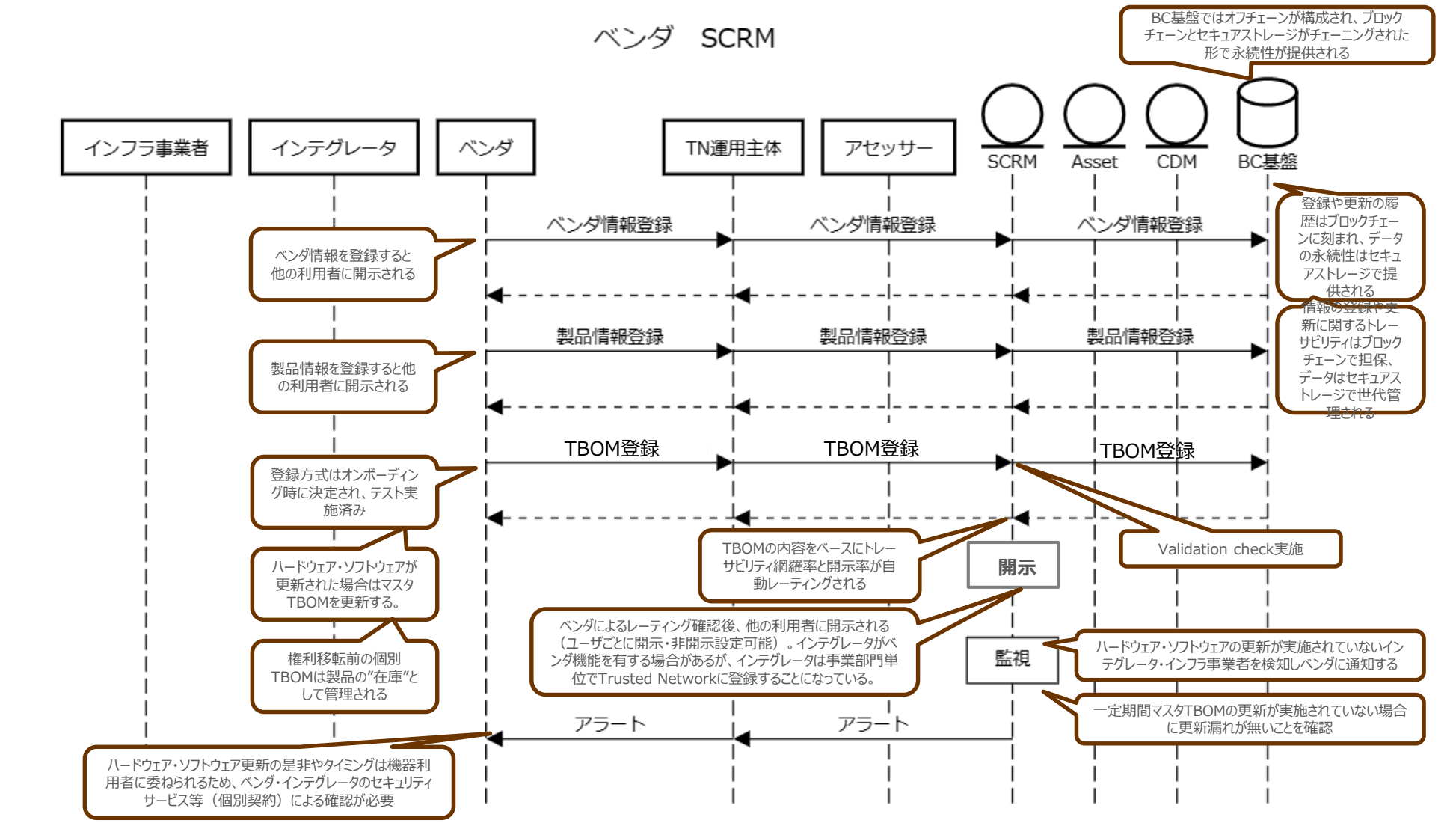
Trusted Networkの構成と機能



CDM: Continuous Diagnostics and Mitigation, H/SBOM: Hardware/Software Bill of Materials, SCRM: Supply Chain Risk Management

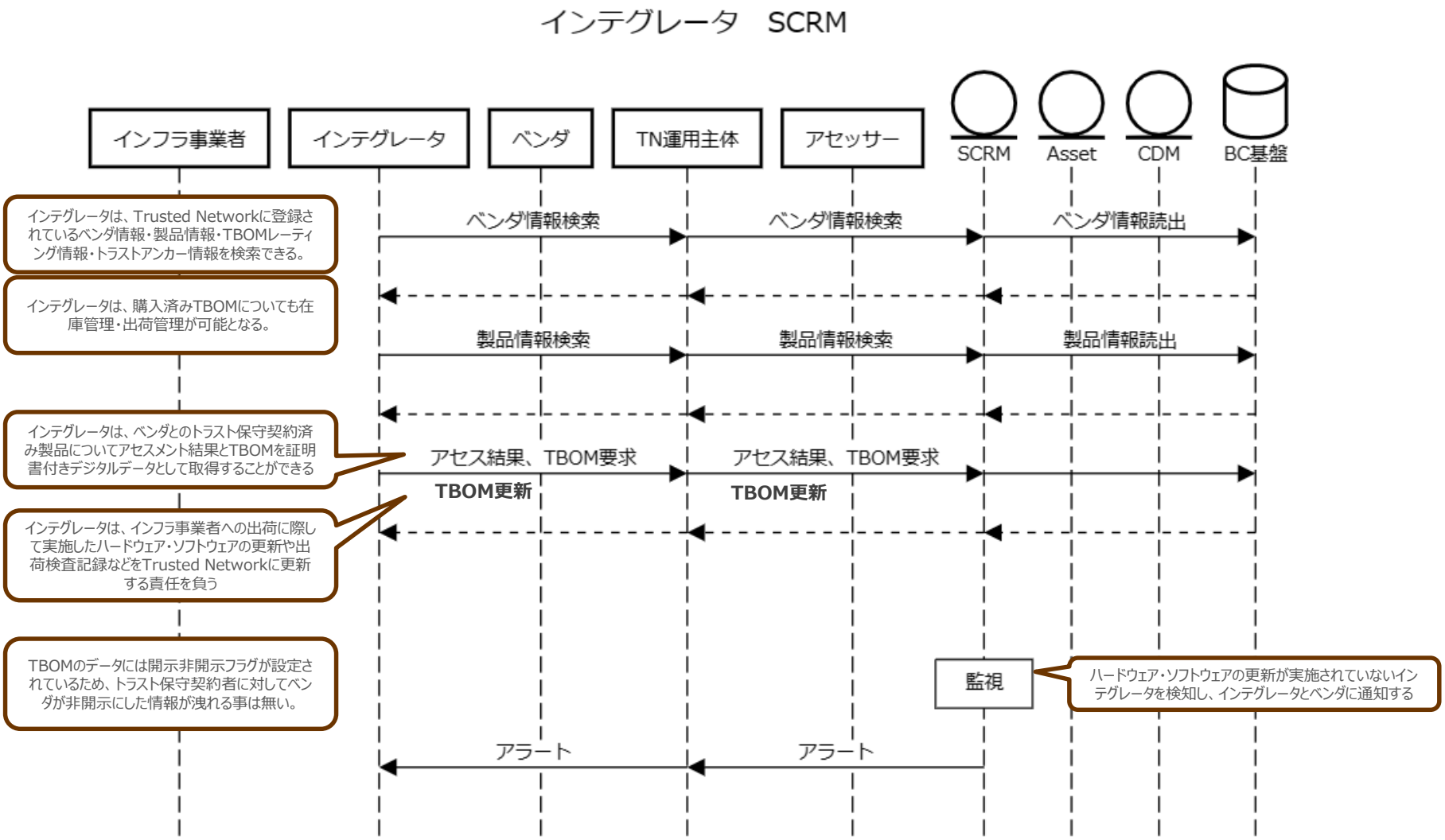
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



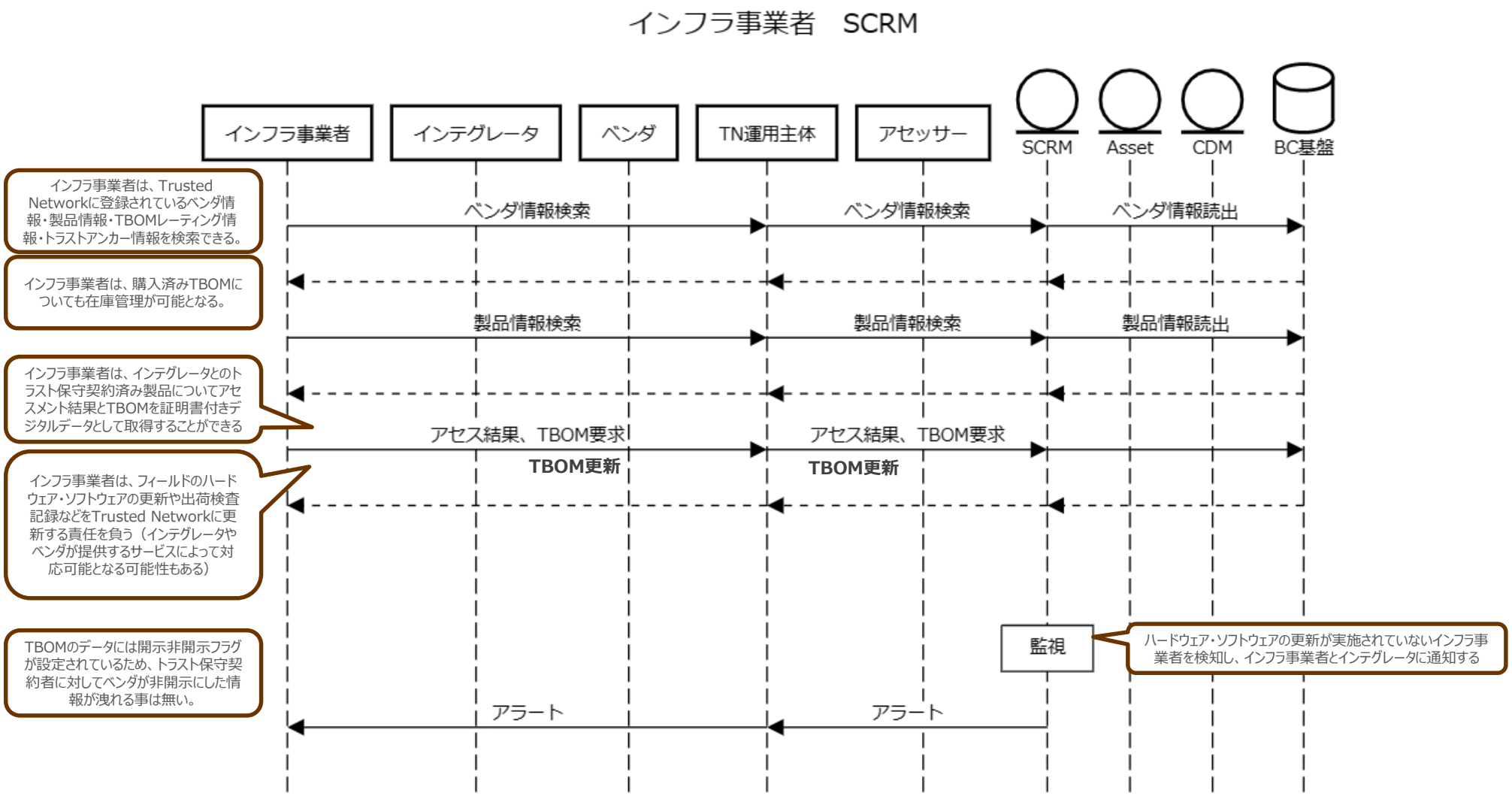
3.4 本実証で企画・開発したシステムの概要（1/6）

業務フロー



3.4 本実証で企画・開発したシステムの概要（1/6）

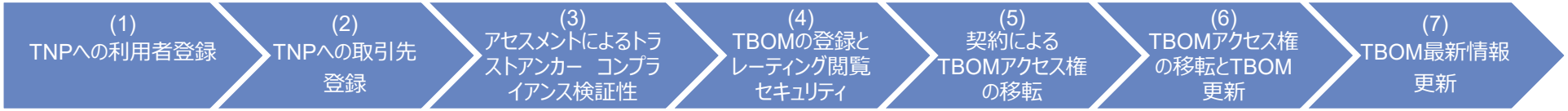
業務フロー



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

Trusted Network（TN）の主要なプロセスについて、ユースケース図で説明する。

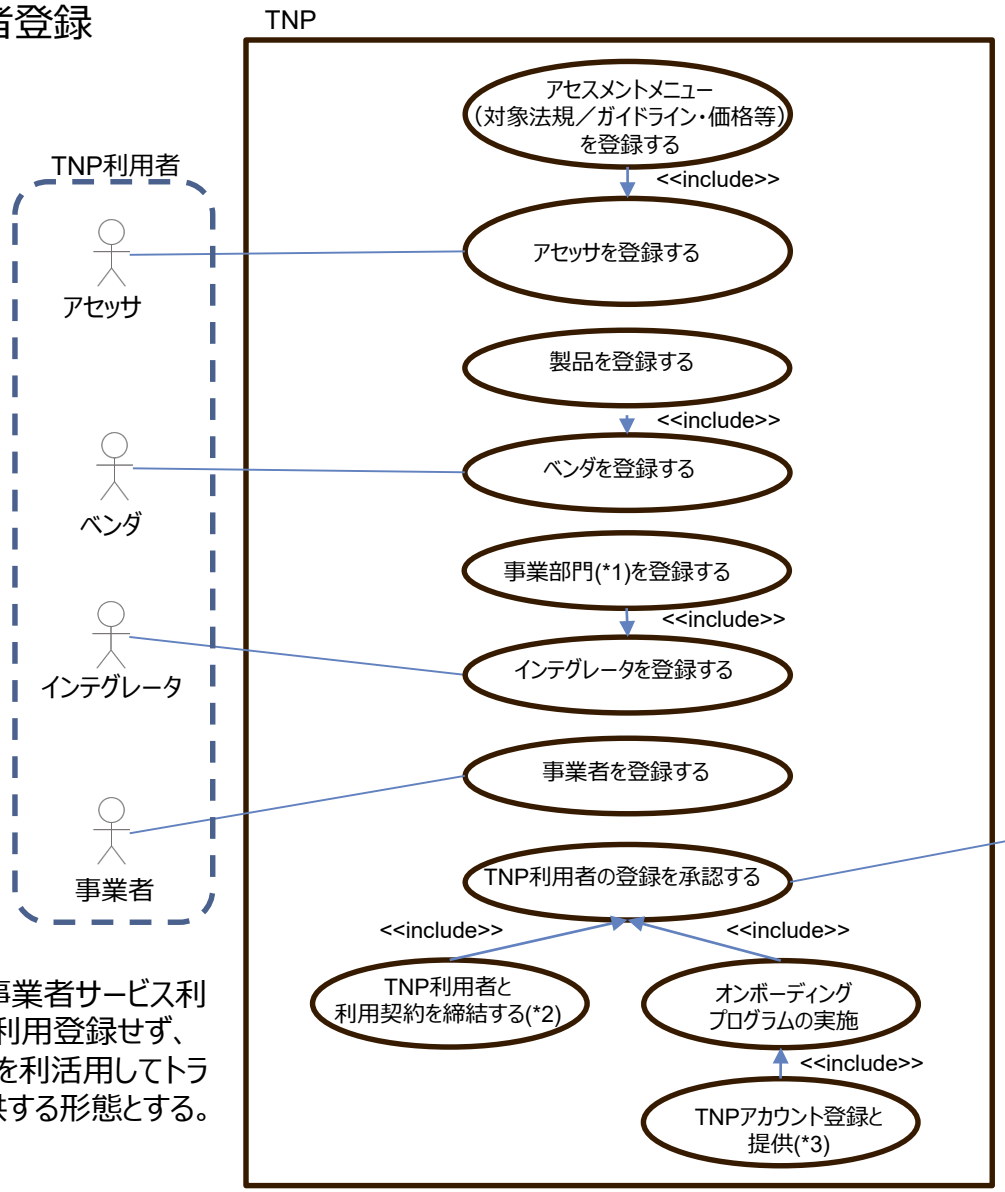


#	プロセス	概要
(1)	TNPへの利用者登録	TNの利用者（ベンダ、インテグレータ、事業者等）を登録
(2)	TNPへの取引先登録	TN上で取引を行う利用者を登録
(3)	アセスメントによるトラストアンカー コンプライアンス検証性	利用者（ベンダ、インテグレータ）のセキュリティ基準への適合度をアセスメントする
(4)	TBOMの登録とレーティング閲覧セキュリティ	ベンダ製品のTBOMを登録し、TBOMの開示度合い・リスク等を基にした情報の評価（レーティング）を閲覧する
(5)	契約によるTBOMアクセス権の移転	ベンダ製品の契約（購入・出荷）に伴うTBOMアクセス権の移転
(6)	TBOMアクセス権の移転とTBOM更新	事業者に製品出荷とともにTBOMの所有権を移転（更新）
(7)	TBOM最新情報更新	事業者に移転したTBOMの情報を最新化（更新）

3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

(1)TNPへの利用者登録



政府・省庁や事業者サービス利用者はTNPに利用登録せず、事業者がTNPを利活用してトラスト情報を提供する形態とする。

(*1): 例えば14の基幹インフラ業種のうち、どの業種に対応する部門なのかを登録

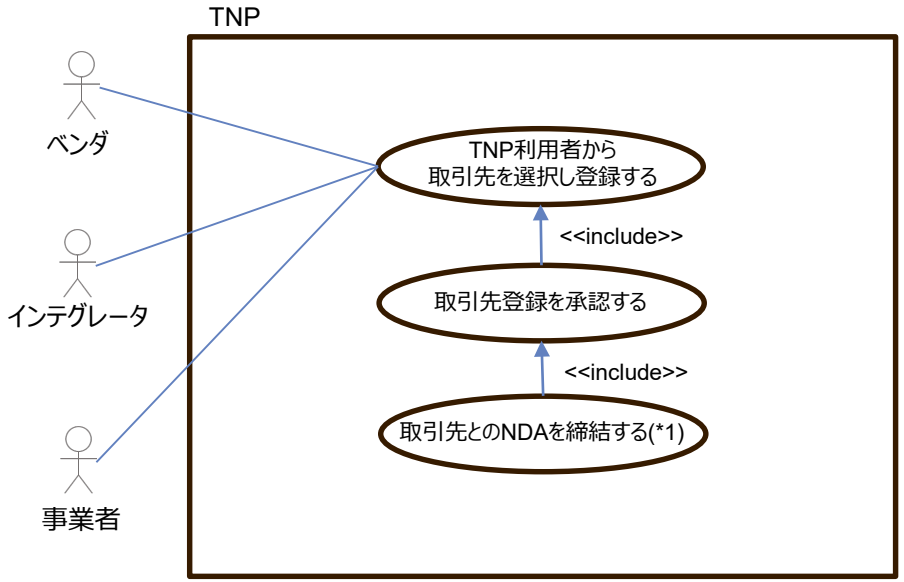
(*2):利用契約の際に事業者の確認を実施する

(*3):TNPへのアカウント登録時にTNP内にdidやウォレットが生成されアカウントと紐づけられる

3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

(2)TNPへの取引先登録



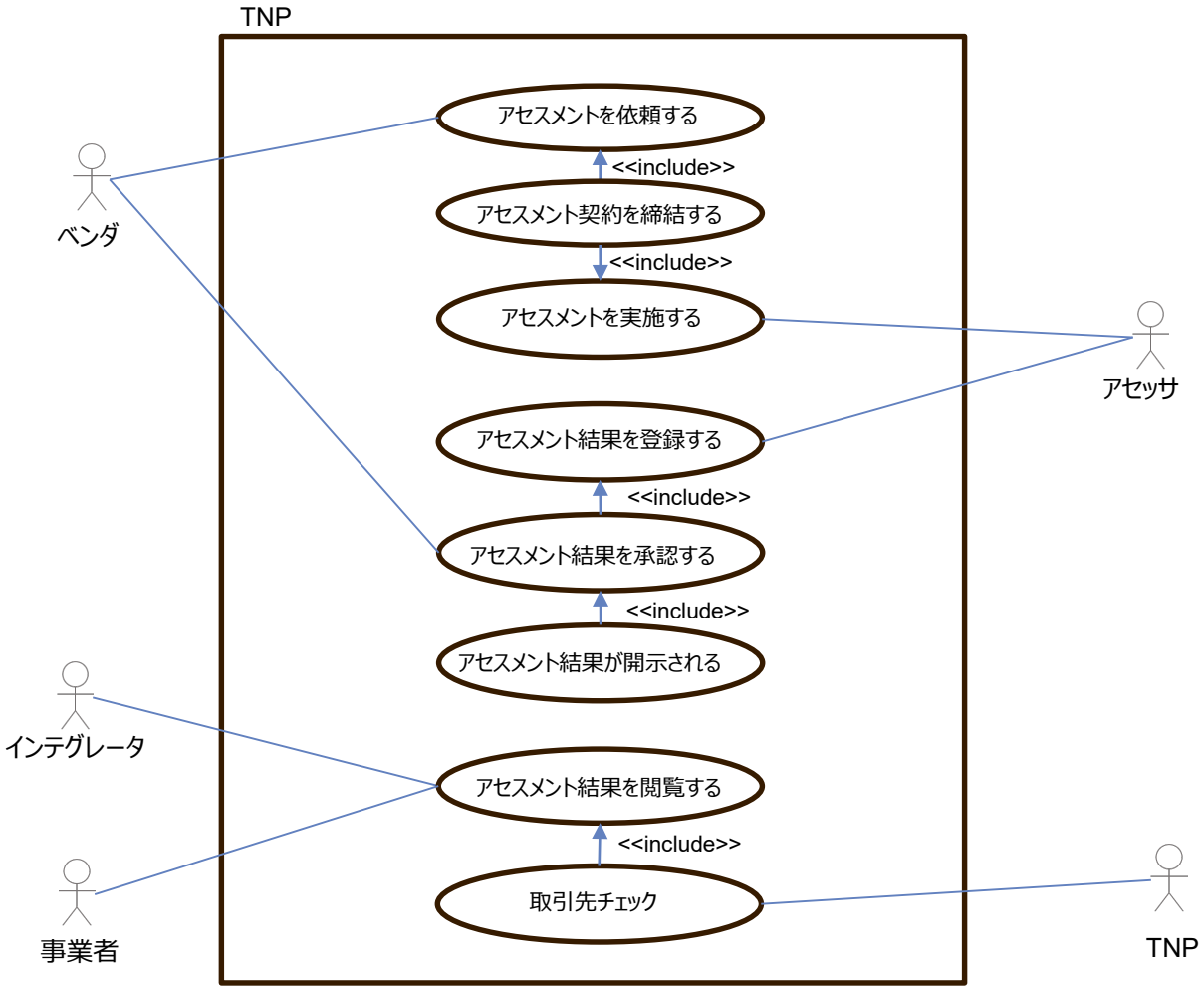
NOTE：アセスメント結果やTBOMのレーティングは
取引先のみに開示される

(*1): NDA締結は従来の契約行為を踏襲し、NDA
締結後に取引先登録を承認するルールとする

3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

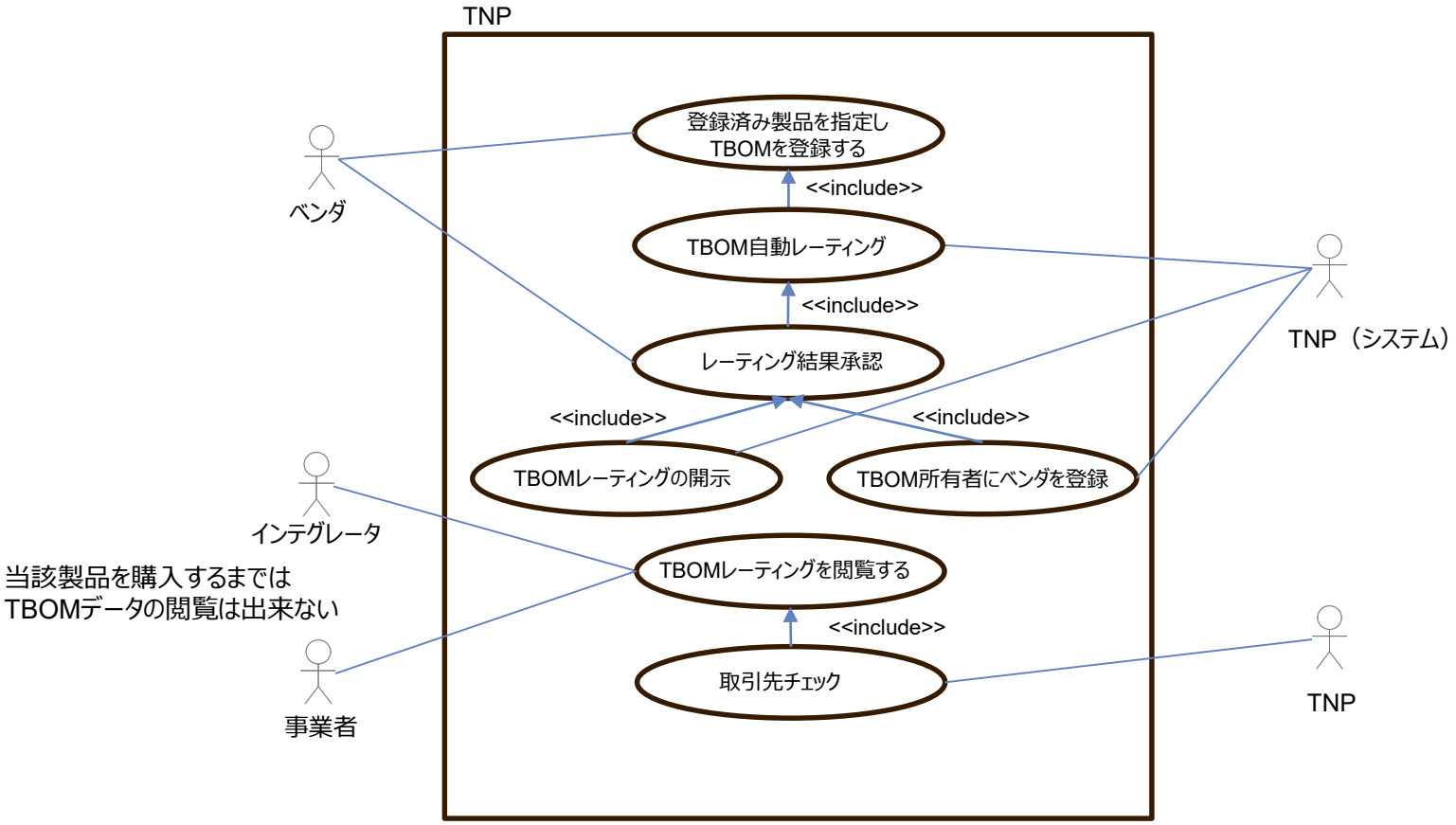
(3)アセスメントによるトラストアンカー　コンプライアンス検証性



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

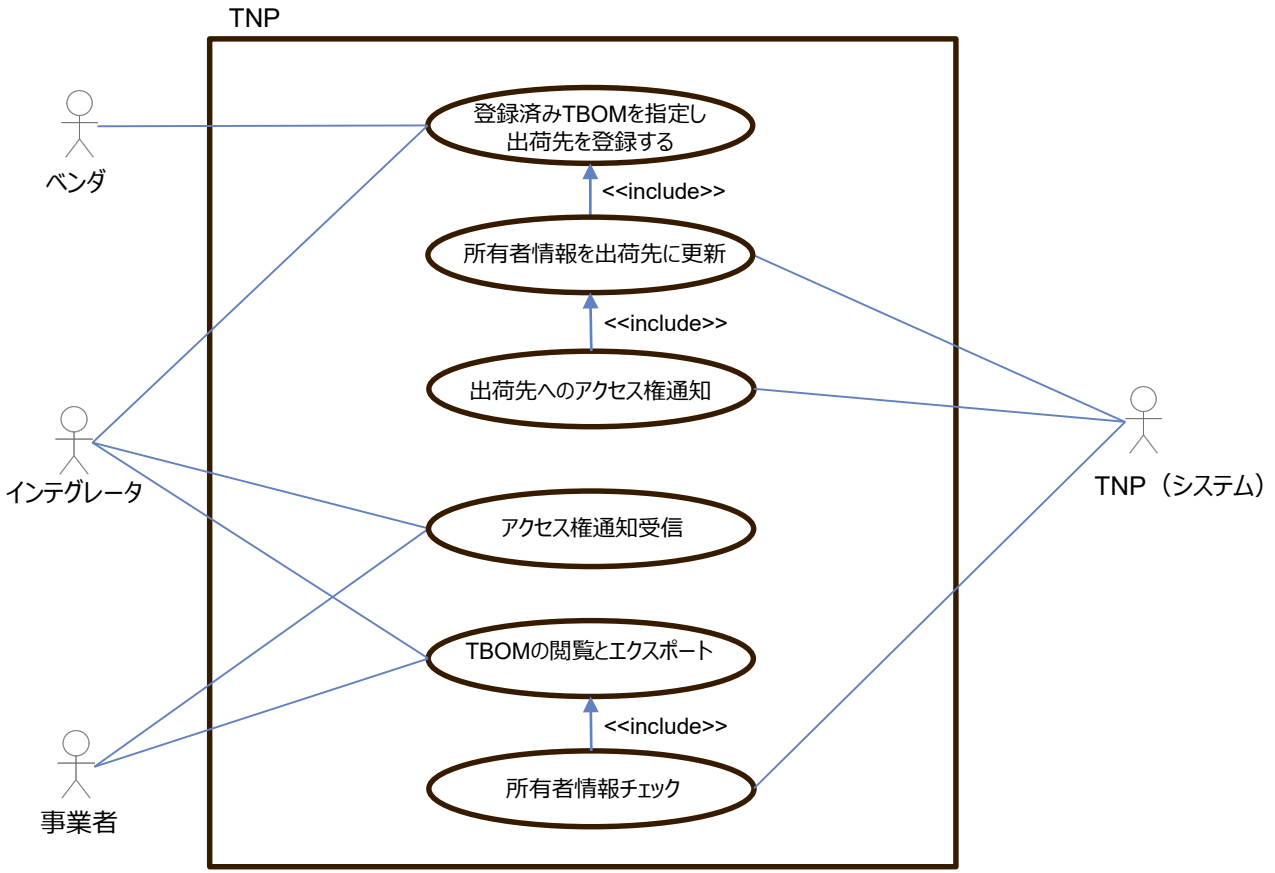
(4)TBOMの登録とレーティング閲覧セキュリティ



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

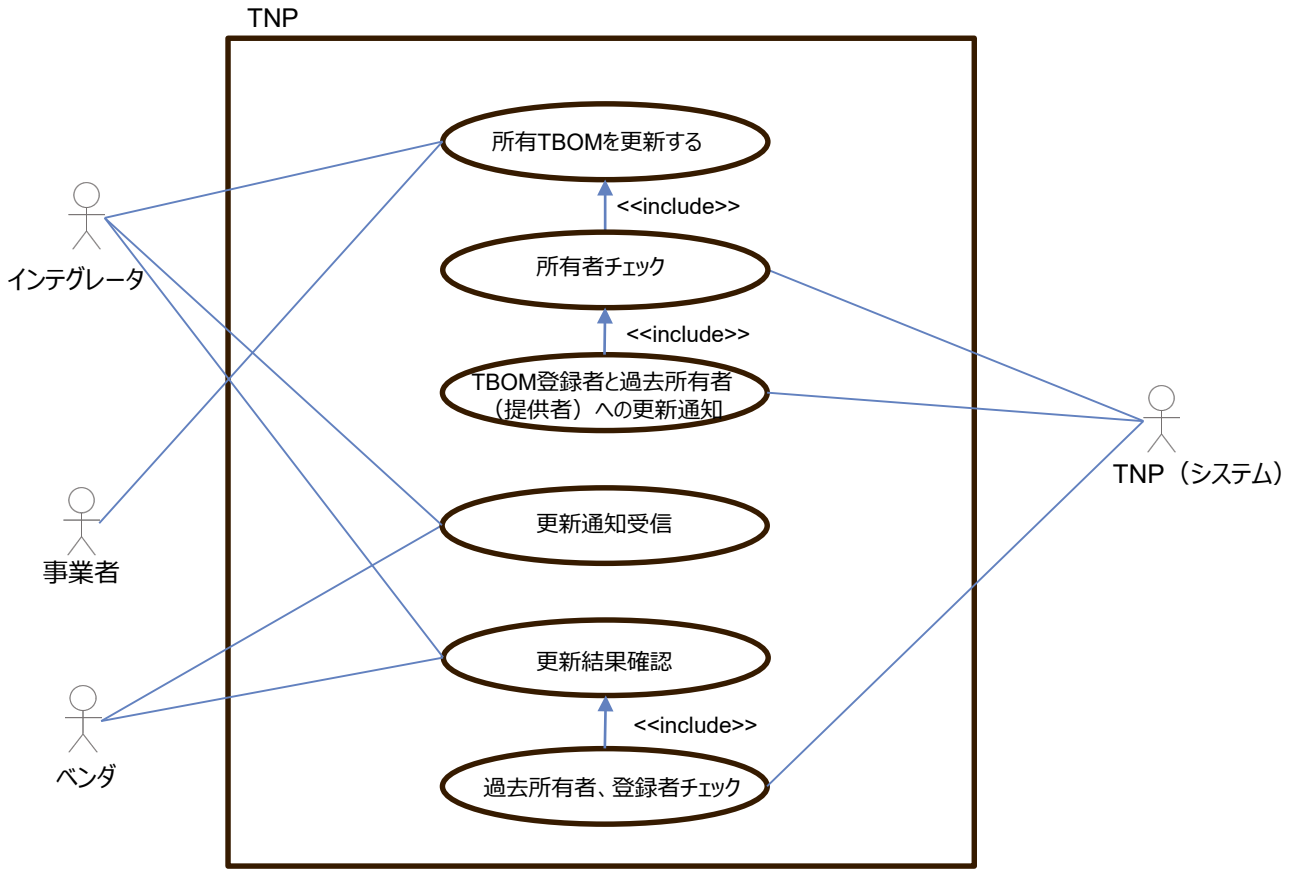
(5)契約によるTBOMアクセス権の移転



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

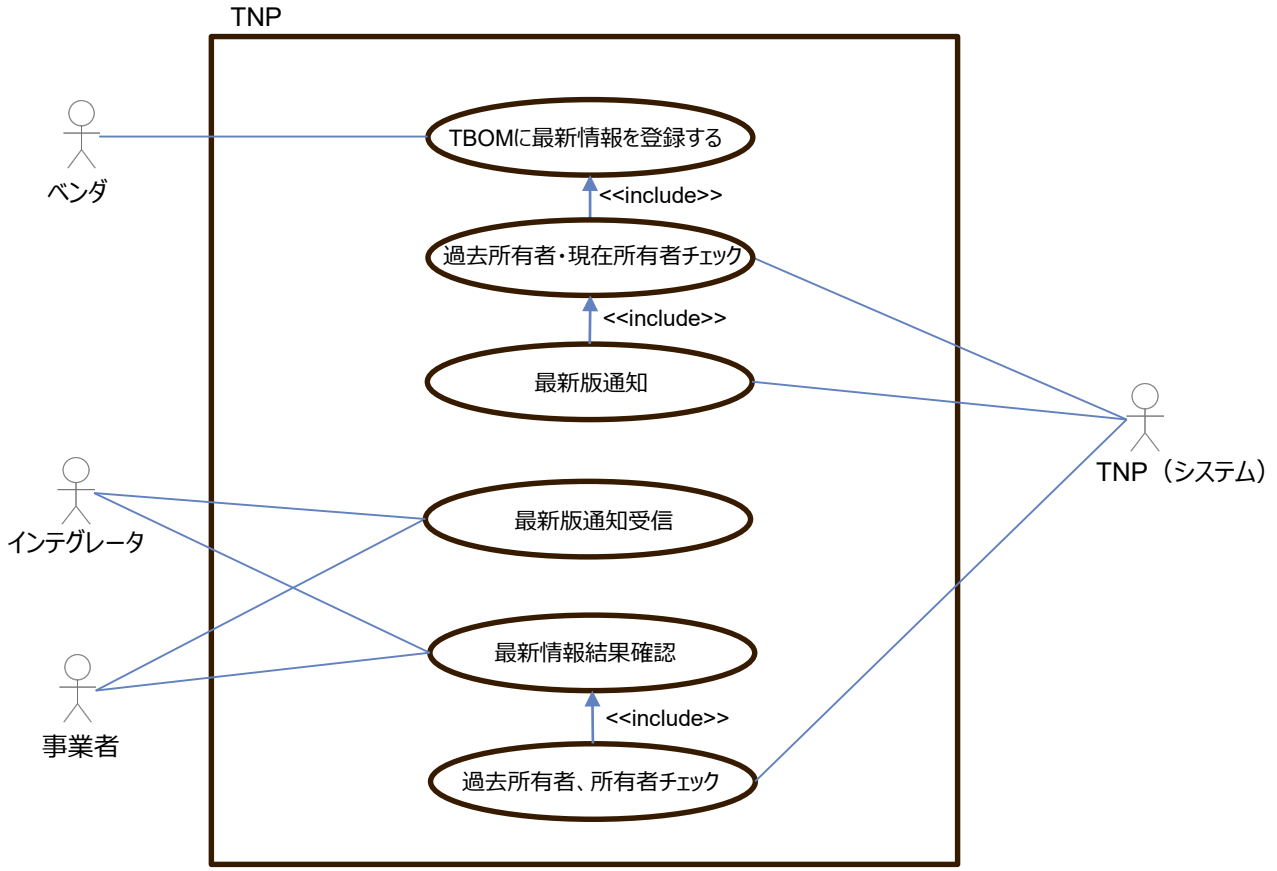
(6)TBOMアクセス権の移転とTBOM更新



3.4 本実証で企画・開発したシステムの概要（2/6）

ユースケース図

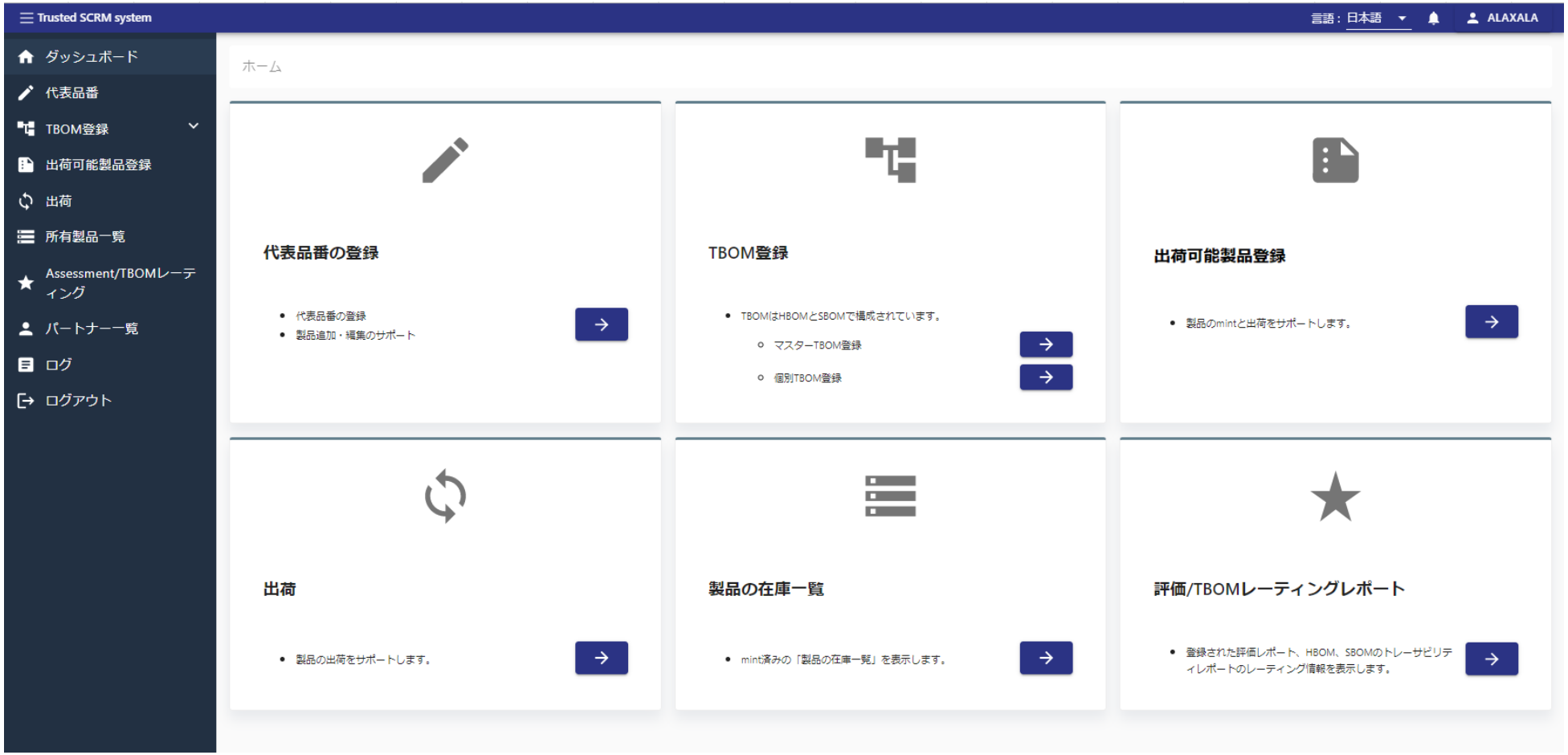
(7)TBOM最新情報更新



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

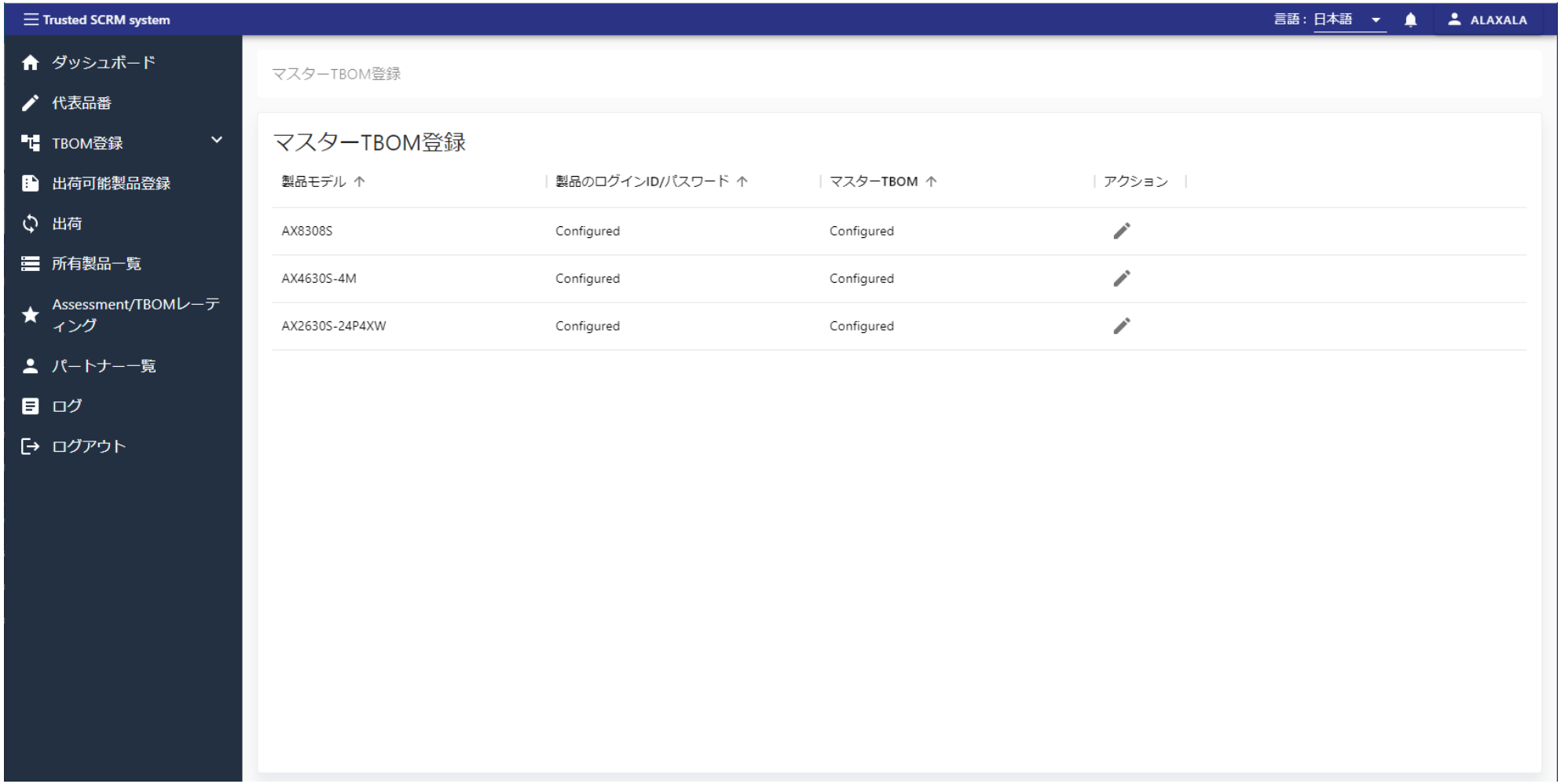
①Trusted SCRMダッシュボード



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

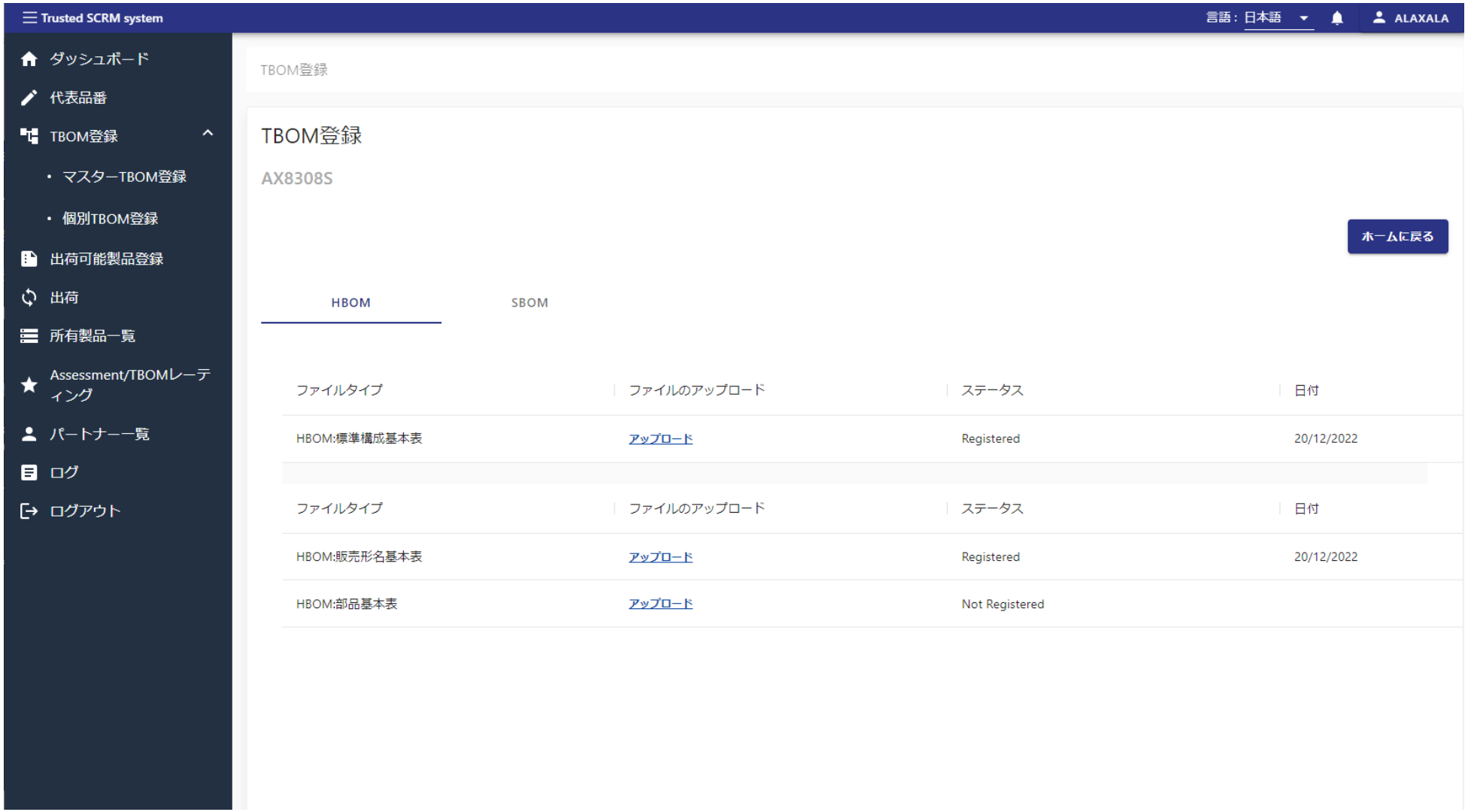
②Trusted BOM (TBOM)の登録（１）



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

②Trusted BOM (TBOM)の登録（２）



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

③アセスメント/TBOMのレーティング（１）

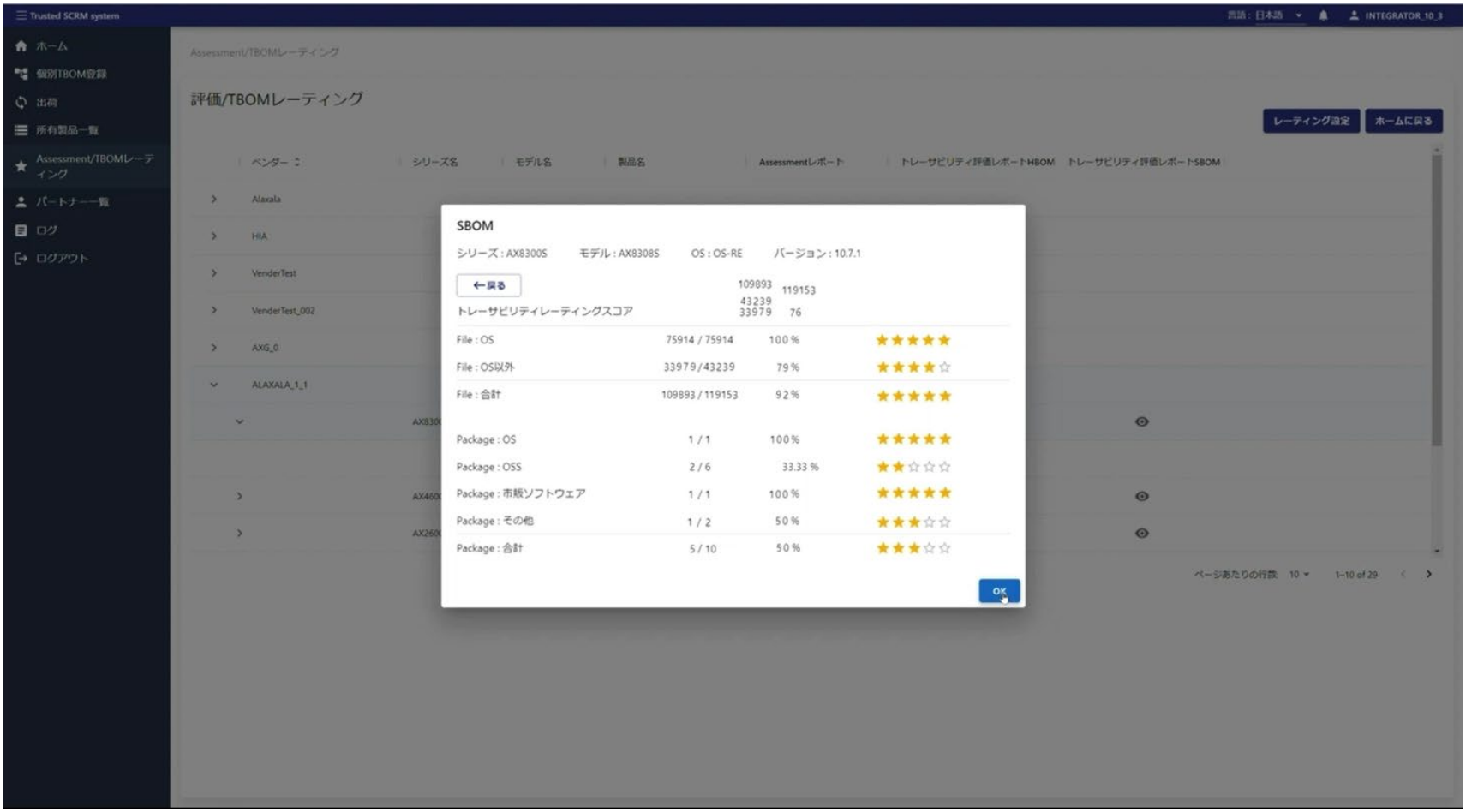
- TNに登録されている全シリーズ・モデルについて、その登録されているTBOMのトレーサビリティ・レーティング情報を参照可能
- ベンダーは自社製品のみ、インテグレータ・インフラ事業者は全ベンダーの製品について参照可能

→ 調達・製品選定に利用可能

3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

③アセスメント/TBOMのレーティング（２）



SBOMのレーティングは、以下の項目ごとの記載率でスコアリング表示 （★の数が多いほど、透明性[開示率]が高いと判断）

- **File： ソフトウェアファイルの種別・用途 （ OS or その他機能 ）ごとにコピーライト情報・入手先（提供元定義）情報、ライセンス定義**
- **Package： ソフトウェアパッケージの種別 （ OS, OSS, 商用パッケージ, その他 ）ごとに入手先（提供元定義）情報、ライセンス定義**

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

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	ベンダ・インテグレータ・事業者・アセッサーは、公益的第三者（Trusted Network運用者）とTrusted Network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、Trusted Network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、Trusted NetworkでTBOMを提供する製品をTrusted Networkに登録する。 登録済み製品の一覧と詳細情報は、Trusted Network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	アセッサーは、自社が提供するアセスメントサービスについてTrusted Networkに登録を行う。登録されたサービスの一覧と詳細情報は、Trusted Network利用者全員が閲覧可能となる。
機能	アセスメント依頼	ベンダ	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	アセッサは、Trusted Network経由でアセッシーからのアセスメント依頼を受理し、当該アセッシー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－アセッシー間のDynamic Consentを生成する。 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 アセッシー	アセッサーは、アセッシー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ーに確認依頼される。
機能	アセスメント結果確認完了、開示	アセッサ アセッシー	アセッシーはアセッサーから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Trusted Network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。

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

<table>
<tr><th>機能/非機能</th><th>機能名</th><th>アクター</th><th>機能概要</th></tr>
<tr><td>機能</td><td>TBOM登録</td><td>ベンダ</td><td>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。
※登録時、TNPFはvalidation checkを実施し、invalid dataについてはエラーとしベンダに通知する。</td></tr>
<tr><td>機能</td><td>TBOMレーティング結果登録</td><td>TNPF</td><td>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。
<table>
<tr><td rowspan="2">網羅性</td><td>ハードウェア</td><td>重要部品点数のうちトレーサビリティが管理できている部品数の割合</td></tr>
<tr><td>ソフトウェア</td><td>重要ソフトウェアのうちSBOMが管理できているソフトウェア数の割合</td></tr>
<tr><td rowspan="2">透明性</td><td>ハードウェア</td><td>重要部品点数のうちトレーサビリティが管理できており、尚且つトレーサビリティを開示できる部品数の割合</td></tr>
<tr><td>ソフトウェア</td><td>重要ソフトウェアでSBOMが管理できているソフトウェアのうち、SBOMを開示できるソフトウェア数の割合</td></tr>
</table></td></tr>
<tr><td>機能</td><td>TBOMレーティング結果確認・開示可否確認</td><td>ベンダ</td><td>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。</td></tr>
<tr><td>機能</td><td>TBOMレーティング開示</td><td>TNPF</td><td>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。</td></tr>
<tr><td>機能</td><td>アセスメント結果、TBOMレーティング閲覧（調達・選定時）</td><td>事業者</td><td>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、Trusted Network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。</td></tr>
</table>

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/非機能一覧

機能/非機能	機能名	アクター	機能概要
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Trusted Network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。

3.4 本実証で企画・開発したシステムの概要（4/6）

機能/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。 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、VCやトレース情報は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　本実証で企画・開発したシステムの概要（5/6）

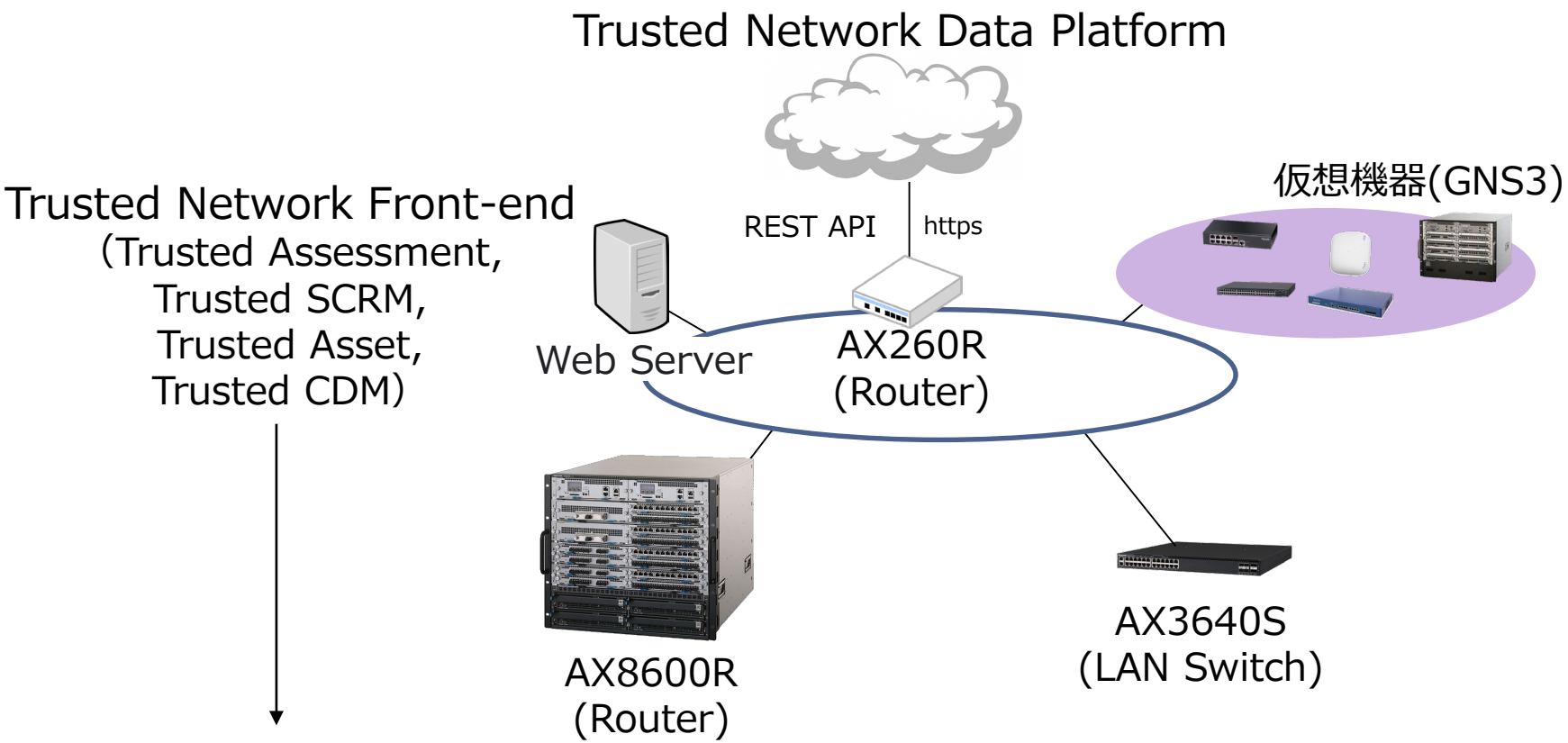
データモデル定義

TNへのベンダ登録時のVC

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 本実証で企画・開発したシステムの概要（6/6）

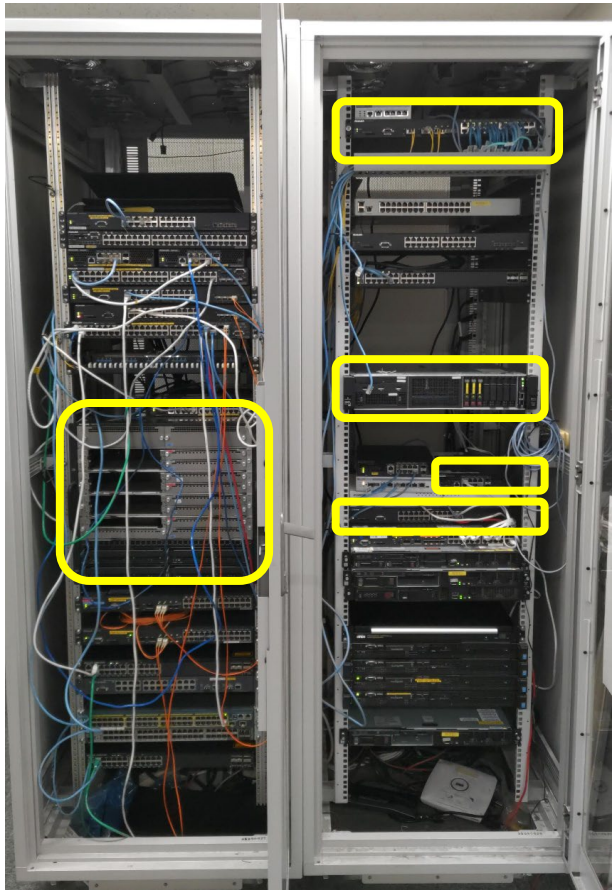
実験環境



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				

3.4 本実証で企画・開発したシステムの概要（6/6）

実験環境



3.5 実証を通じて得られた主な成果

システムの企画・開発に関する成果

- Trusted Webユースケースの創出・実証
  - Trusted Webのユースケースとして、IT機器調達においてサプライチェーン上でIT製品の真正性確認を行う仕組み（Trusted Network）を検討、企画した
  - Trusted Web要件に整合するTrusted Networkの機能仕様を検討した

- Trusted Webユースケースのプロトタイプ
  - Trusted Networkのプロトタイプを自主事業で開発し、沖縄オープンラボラトリにてプロトタイプによる価値実証（POV: Proof of Value）を実施した。
  - Trusted Webの要件を満たすシステムとして、実際に想定通り動作することを実証した。
  - 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が解決される可能性を実証した。

ビジネスモデルに関する成果

- エコシステム型のビジネスモデルを検討
  - Trusted Network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て実現するエコシステム型のビジネスモデルを考案した。
  - Trusted Networkのプラットフォームの運用主体（TNSP）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。

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

- アラクサラは本実証事業をB類型で受託しており、プロトタイプの開発をすべて自社費用で実施した。
- 他者が、同様なシステムを記載した要件にしたがって再現することは可能と考える。

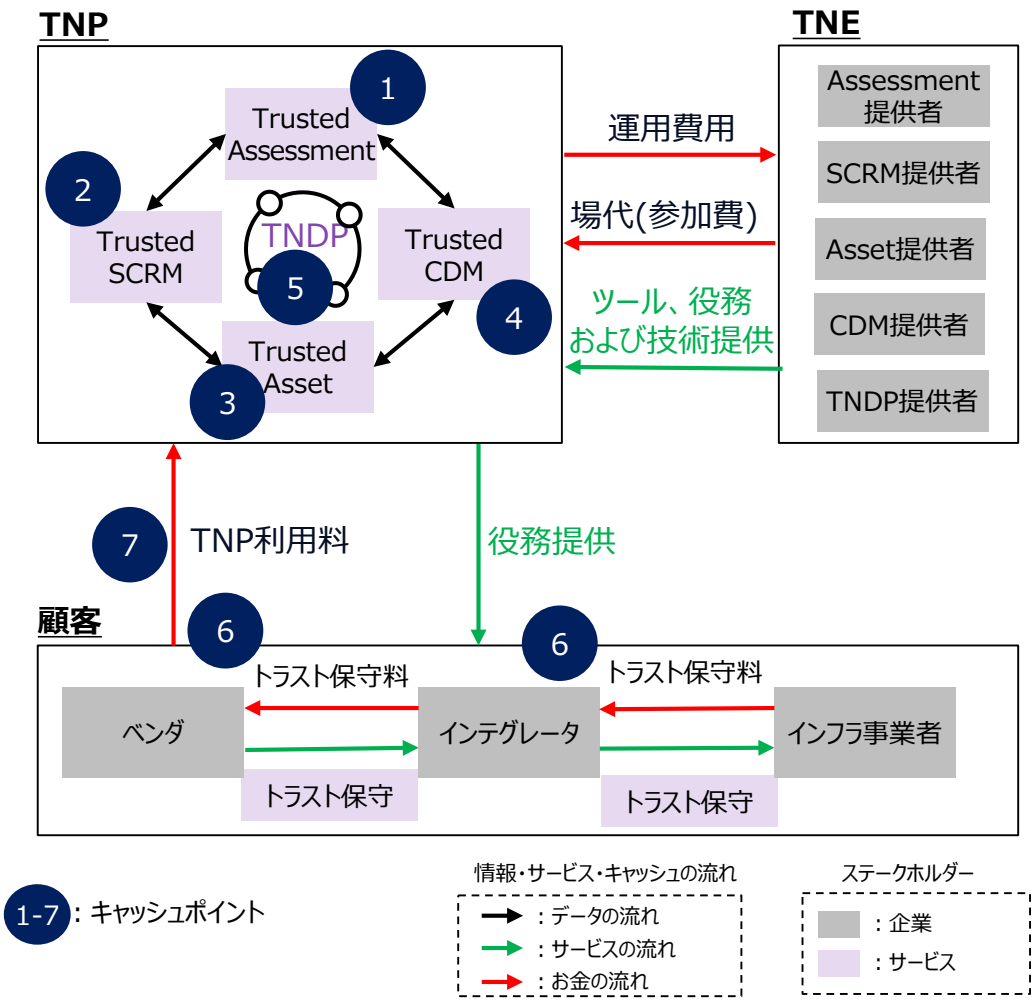
  ただし、開発投資は少なくとも数億円以上に及ぶため、同様な投資をするくらいなら、エコシステム・パートナーとしてTrusted Network構想に参画して、共創していくほうが、コスト的にも、複数方式並立による混乱をさけるためにも、望ましいと考える。
- また、Trusted Networkの基本的なコンセプトや方式は、今回の受託の前から検討、知財を考案済であり、ライセンスの利用については検討中である。

04

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

ビジネスモデル



ユーザーのベネフィット

ステークホルダ	ベネフィット	負担するコスト
TNP (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
インフラ事業者	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 • トラストBOMの維持・運営費
インテグレータ	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（場代） • トラスト保守費 • トラストBOMの維持・運営費 • 技術・ツール費

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

課金モデル・キャッシュポイントについて

（1）PF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、ベンダーの値段設定が高いと、インテグレーター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、ユーザーと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。

<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="4">-</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>

TNE: Trusted Network Enabler (Trusted Networkサービス提供の協力企業・機関)

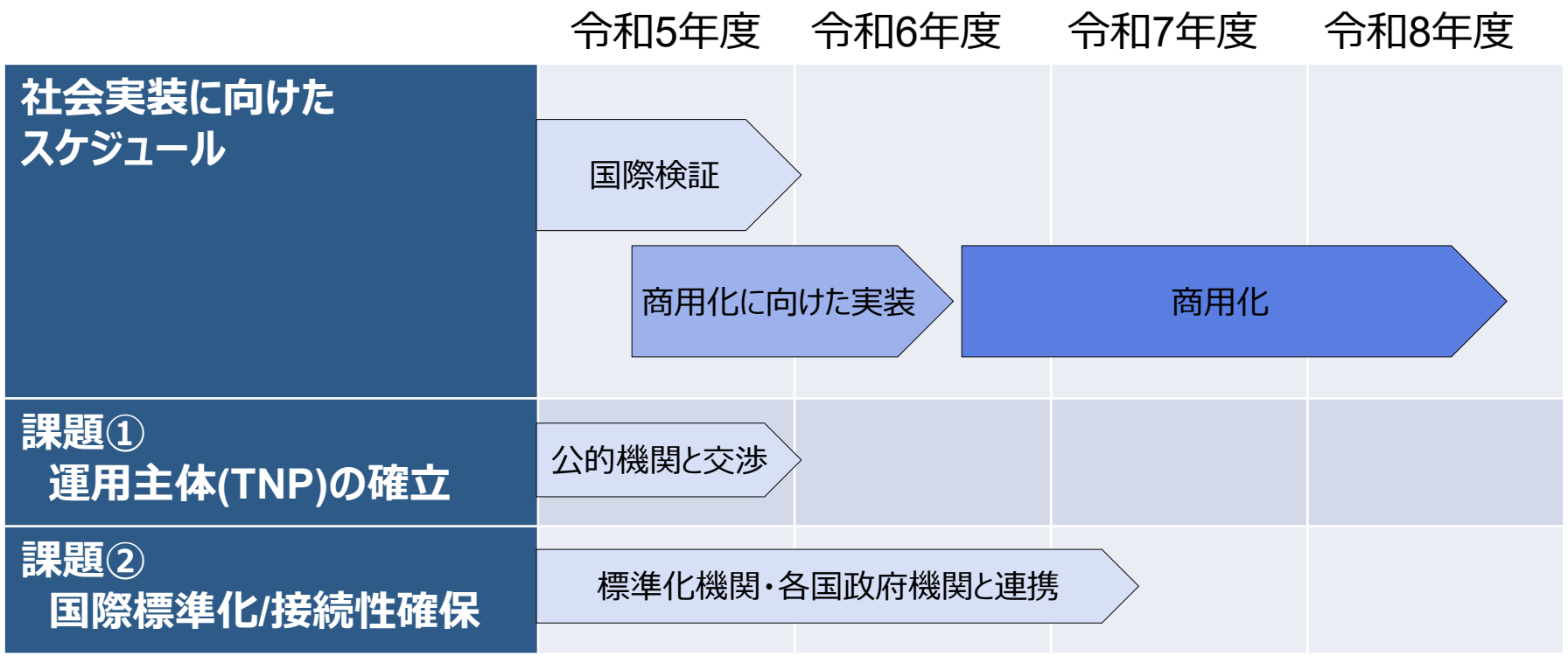
4.2 実証を通じて判明したユースケースの課題とその解決方針

#	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政府機関のキーマンとの対話を実施、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た

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

#	実現上の課題	対応方針/対応状況
5	Trusted Networkを管理・運用する主体（組織体）の立上げ	Trusted Network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	Trusted Network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Trusted Network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	Trusted Network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

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



05

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

アーキテクチャ及び技術

（1）現状認識と課題

- Trusted Webの実現に向けては、実装アーキテクチャやデプロイメント設計についての具体記述が不足
- 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不明。
- Trusted Webホワイトペーパー 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、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は理解しづらく、混乱を招く
- 敢えてこのように記載しているのは承知しているが、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、示すべき段階と考える。
- 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、事態を集約するためのコスト増大が懸念される）

（2）示唆と提言

- 以下のような記述の追加を提案したい。

「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トロコルであり、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 Trusted Webのアーキテクチャに関する課題と提言

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、トラストを確保するためには、実際にデータをやり取りする前の段階と、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と考える。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Trustを高めるアプローチは必要十分とは言えないため。
- Trusted Network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、Trusted Network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

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、トラストはコストである。
- Trusted Webの実装にかかるコスト、運用にかかるコストは誰がどのように負担するのか。
- 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。
- 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真となる。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　その他Trusted Webの課題と提言

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案が示されることが望ましい。リアリティが上がることでユースケースもより実践的な提案がなされるものと考える。また同様の理由で、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ることが望ましい

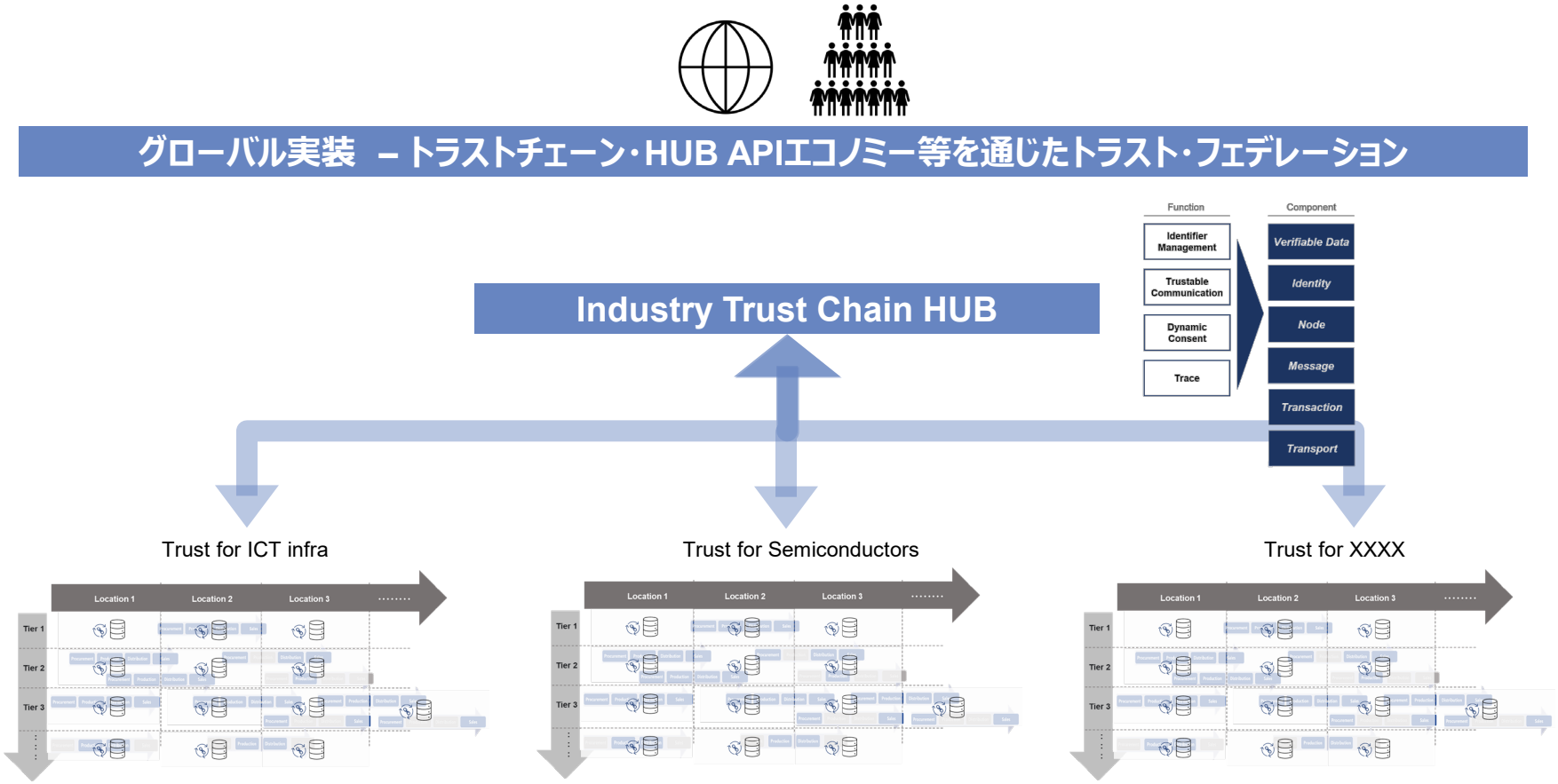
（２）示唆と提言

- 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。
- 次ページにグローバル連携、業界横断の連携スキームの提案を示す

5.2 その他Trusted Webの課題と提言

政策とグローバリゼーション

- 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」の実現に向けた国際標準化の推進
- Trusted Webを適用したユースケースの先行規格化を行い、他とのTrusted Web事例との整合をすすめていくべき



付録

1.用語集

2.Trusted Webの要件ごとの対応機能と課題

3.Trusted Networkにおけるプレーヤの定義・役割

4.関連標準規格

用語集（１）

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
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も制定している。
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
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

用語集（2）

用語	定義
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
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「状態」や「場」を指す。 「多様な構成員の相互協力および平等な収益の循環が、エコシステムを健全に機能させる条件」
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。「リーダ企業の構想力に依存」
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
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。

Trusted Webの要件ごとの対応機能と課題（要件１）

要件１．ユーザ自身が自らに関連するデータをコントロールできる

（１）Trusted Networkへのユーザ登録

- Trusted Networkでは、主体者の登録に際して、利用契約に連動しW3Cに準拠したDIDを発行する
- DIDには、主体者の登録（属性）情報が紐づけられてTrusted Networkに登録される

（２） Trusted Networkへの製品およびトラストBOM情報の登録

- Trusted Networkでは、製品およびトラストBOMの登録に際して、それぞれにDIDを発行する
- DID情報として、ベンダのDID、製品のDID、トラストBOMのDID、トラストBOMのIPFSのパス、ベンダの署名をブロックチェーンに記録し、トラストBOM情報の開示設定（可否、対象、条件）を可能

課題：

Trusted Networkを管理・運営し、DID/VCを発行する「公益的な第三者」が必要。現実的には政府・公的機関の関与が必要になりそうだが、これが立ち上げられないと成立しない。**Trusted Networkの運営主体がどうあるべきか**を整理することが課題。

要件１に対するTN機能　-　ユーザ登録、トラストBOM登録

要件１．ユーザ自身が自らに関連するデータをコントロールできる

- Trusted Networkでは、主体者の登録に際して、利用契約に連動しW3Cに準拠したDIDを発行する。
- DIDには、主体者の登録（属性）情報が紐づけられており、正規の資格を有する主体しかその登録情報を参照できない仕組みになっている

TNSにおけるユーザー登録手順

1. TNS利用希望者は必要情報を入力してサービス登録申請を行う
    a. ベンダ、インテグレータ、オペレータ、アセッサ、政府ユーザは共通
        i. それぞれの役割として権限が設定される
2. Trusted Networkを運営する公益的な第三者は登録申請を確認する
    a. 公益的な第三者も管理者の役割を持つ1ユーザとして管理されている
3. 公益的な第三者が登録申請者に対してユーザー登録としてDIDを生成する　DID
    a. ウォレットを生成する
        i. ウォレットアドレスをDIDの識別子として設定する
    b. 登録情報をDID識別子に紐付けてIPFSにアップロードする
        i. 公益的な第三者がユーザのVC発行　VC
    c. アップロードした記録をブロックチェーンに記録する

要件１に対するTN機能 - ユーザ登録、トラストBOM登録

要件１．ユーザ自身が自らに関連するデータをコントロールできる

- Trusted Networkでは、製品およびトラストBOMの登録に際して、製品、トラストBOMにDIDを発行する。
- DIDには、主体者の登録（属性）情報が紐づけられており、正規の資格を有する主体しかそのトラストBOM情報を参照できない仕組みになっている

TNSにおける製品登録手順

1. 必要な情報をアップロードもしくは手入力する
   a. データをIPFSに記録する
   b. 登録や更新の履歴とデータのパスはブロックチェーンに記録される Trace
2. データ登録の際に得られる識別子を元にDIDを生成 DID
3. DID情報をブロックチェーンに記録する
   a. ベンダのDID
   b. 製品のDID
   c. 製品情報のIPFSのパス
   d. ベンダの署名
4. ベンダが製品情報のVC発行 VC

トラストBOMの登録手順

1. 必要な情報をアップロードする
   a. データをIPFSに記録する
   b. 登録や更新の履歴とデータのパスはブロックチェーンに記録される Trace
2. データ登録の際に得られる識別子を元にDIDを生成 DID
3. DID情報をブロックチェーンに記録する
   a. ベンダのDID
   b. 製品のDID
   c. マスタートラストBOMのDID
   d. マスタートラストBOMのIPFSのパス
   e. ベンダの署名
4. ベンダがマスタートラストBOMのVC発行 VC
5. 情報公開設定を行う
   a. データを公開するか否か
   b. データ公開対象
   c. データ公開条件

Trusted Webの要件ごとの対応機能と課題（要件２）

要件2．検証(verify)できる領域を拡大することにより、Trustの向上を図ることができる

（１）Trusted Networkへのユーザ登録

- Trusted Networkに参加する各主体は、取引先の主体の属性情報を各主体に問合わせることなく、Trusted Networkから参照可能。

（２）Trusted Networkへの製品およびトラストBOM情報の登録

- Trusted Networkに参加する各主体は、自らの属性に応じて、取引先(候補)のベンダの製品のトラストBOM情報をベンダに問合わせることなく、Trusted Networkに登録された製品およびトラストBOM情報を参照可能。

（３）アセスメント結果の登録と利用

- ベンダの製品に対して、トラストアンカー（アセッサー)がアセスメントを実施し、その結果を対象製品と連携させ、Trusted Networkにアップロード、製品およびTBOMのVCを発行する。アセスメントの保存履歴はブロックチェーンに記録し、改ざんできない。アセスメント結果は、ベンダが開示可否、開示対象の指定/限定、開示条件を設定する。
- インテグレータ/事業者は、設定された権限、開示条件に基づき、リアルタイムにアセスメント結果を閲覧、検証することが可能で、Trustの度合いを検証できる。

要件２に対するTN機能　-　アセスメント結果の登録

要件２．検証(verify)できる領域を拡大することにより、Trustの向上を図ることができる

- ベンダの製品に対して、トラストアンカー（アセッサー)がアセスメントを実施し、その結果を対象製品と連携させ、Trusted Networkにアップロード、製品およびTBOMのVCを発行する。アセスメントの保存履歴はブロックチェーンに記録し、改ざんできない。アセスメント結果は、ベンダが開示可否、開示対象の指定/限定、開示条件を設定する。

アセスメント結果の登録

1. ベンダはアセッサを指定してアセスメントを依頼する
2. アセッサはベンダの製品及びマスタートラストBOM情報をアセスメントする
3. アセッサはアセスメント結果を保存
    a. アセッサのシステムと連携
    b. アセスメント結果はIPFSにアップロード
    c. アセッサが製品及びマスタートラストBOMのVCを発行　VC
    d. アセスメント保存履歴はブロックチェーンに記録　Trace
4. ベンダはアセスメント結果を確認して承認/非承認/再依頼を行う　DC
    a. 情報公開設定を行う
        i. データを公開するか否か
        ii. データ公開対象
        iii. データ公開条件

DC: Dynamic Consent

Trusted Webの要件ごとの対応機能と課題（要件３）

要件３．データのやり取りにおける合意形成の仕組みがある

（１）製品アセスメント結果およびトラストBOM情報による動的な合意形成

- ITインフラの調達に際し、事業者は製品アセスメント結果やトラストBOM情報を事前検証することができ、動的にインテグレータ/ベンダと購入の合意形成が可能。
- 主体者の合意形成に応じて、データ利用権及びアクセス権を移転する
- TNに登録された製品アセスメント結果やトラストBOM情報は、ベンダが設定したデータの開示設定（可否、対象、条件）に基づいて、条件が満たされた場合にのみ開示される。

要件３に対するTN機能　- 製品個別トラストBOMの登録,ベンダの発送

要件３．データのやり取りにおける合意形成の仕組みがある

- ITインフラの調達に際し、事業者は製品アセスメント結果やトラストBOM情報を事前検証することができ、動的にインテグレータ/ベンダと購入の合意形成が可能。

[発送準備]

1. 製品個別トラストBOMの登録
    a. 登録方法はベンダ毎に定める（例：CSVアップロード）
    b. 登録タイミングは契約時でも可
2. 開封検知ICラベル貼付
    a. 開封検知ICラベルは事前に準備
    b. Trusted Networkを運営する公益的な第三者が発送（Optional）
3. 真正確認NFT生成
    a. 多要素認証情報の登録
        i. 製品シリアル番号
            1. リーダーでバーコード読み取りを想定（例）SE1-BUB-C
        ii. 開封検知ICラベル情報
            1. リーダーで読み取りを想定（例）SE1-BUB-C
        iii. 論理NFTの紐付け
            1. 論理NFTに製品シリアル番号の紐付け
        iv. 製品個別トラストBOMからHW/SW情報をIPFSに登録
            1. シリアル番号をキーに該当の製品個別トラストを特定する

[発送]

1. 物流のシステムと自動連携
    a. 連携できない場合はベンダ側で入力する
2. 論理NFTを発送先に送信（transfer）する
    a. 所有者の変更
3. 真正確認NFTを物流会社に送信（transfer）する
    a. 着荷時に物流会社から発送先に送信（transfer）する
4. トレーサビリティー情報をブロックチェーンに記録する

Trace

※ 開封検知ICラベル

※ リーダライター

※ シャーシ型スイッチ：AX8300S

Trusted Webの要件ごとの対応機能と課題（要件４）

要件４． 合意の履行のトレースができる

（１）トラストBOM情報の利用権移転及び参照履歴の閲覧

- 主体者間の合意に基づきデータ利用権及びアクセス権を移転した履歴を記録、参照が可能
- 自社が提供したトラストBOM情報の漏洩や不正利用を防止するため、各主体がコントロールするデータの利用権の移転やアクセス状況をトレースし、必要に応じて利用の遮断が可能
- 合意形成履歴とデータアクセス履歴をTrusted Networkに記録
- ブロックチェーンに以下の情報を記録し、権限をもつユーザ(DIDで識別)が履歴の確認（トレース）を行うことを可能とする。またTBOM、製品の所有権移転もトレース可能
  - ユーザの登録情報、更新履歴
  - TBOMの登録や更新の履歴とデータのパス
  - アセスメント保存履歴
  - 製品の発送（所有権移転）

課題：

Trusted Network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**。合理的に受け入れられる真正性確認の対応レベルの検討が課題

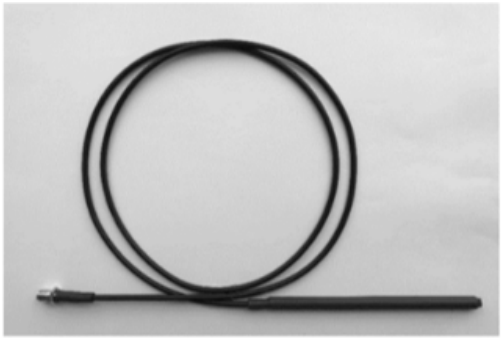
要件4に対するTN機能 - TNにおける真正性確認（１）

- Trusted Assetシステムで管理
- 機器が設定された後のユースケース

1. 開封検知ICラベル情報の読み取り
    a. Trusted AssetシステムからICラベルを取得する
    b. ケーブルアンテナ
        i. 例）CXPA 1.5D SMAJ / CXPA 1.5D SMAP
    c. リーダライター
        i. 例）ImpinjR700 IPJ-R700-441 / MRU-F5100JP
2. シリアル情報及びHW/SW情報の読み取り
    a. Trusted AssetシステムからCLIコマンドから取得する
3. Trusted Assetシステムから真正性確認リクエストを送る
    a. リクエストする真正性確認要素
        i. 製品シリアル番号
        ii. 開封検知ICラベル情報
        iii. HW/SW情報の読み取り
    b. 定期実行、都度実行が可能

※リーダライター

※リーダライター



※ケーブルアンテナ

要件4に対するTN機能 - TNにおける真正性確認（２）

Trusted Network Data Platformでの真正性確認手順

1. 真正確認NFT生成時の要素と送られた要素が全て一致するか突合する
    a. 真正確認NFTの真正確認機能で確認
2. 真正性確認を行ったユーザと論理NFTの所有者が一致するか突合する
    a. 真正確認NFTの真正確認機能で確認
3. HW/SWが一致するか突合する
    a. IPFSに登録されたHW/SW情報と送られたHW/SW情報の確認
        i. ハッシュ比較より情報比較の方がエラー箇所を指摘できるため

※開封検知ICラベルが貼られていなければ（真正確認NFT生成時に登録されていなければ）、開封検知ICラベル情報を送らなくても真正性確認が可能

情報セキュリティ関連国際標準

標準化団体	委員会	ワーキンググループ	標準	内容
ISO	TC 292（セキュリティ及びレジリエンス技術専門委員会）	-	ISO 22301	社会セキュリティ. – 事業継続マネジメントシステム – 要求事項
		-	ISO 22313	社会セキュリティ–事業継続マネジメントシステム–手引
	-	-	ISO 31000	リスクマネジメント
IEC	TC 65	-	IEC 62443	制御システムのセキュリティ
ISO、IEEE共同策定	-	-	IEEE P1363	公開鍵暗号
ISO/IEC JTC	SC 27情報セキュリティ	WG1情報セキュリティマネジメントシステム	ISO/IEC 27000 ファミリー	情報セキュリティマネジメントシステム（ISMS）
		WG2暗号とセキュリティメカニズム	ISO/IEC 18033	
		WG3セキュリティ評価基準	ISO/IEC 15408	コモンクライテリア
			ISO/IEC 18045	CEM (Common Evaluation Methodology : 共通評価方法)
		WG4セキュリティコントロールとサービス	ISO/IEC 27030 ファミリー	
		WG5アイデンティティ管理とプライバシー技術	ISO/IEC 24760ファミリー	アイデンティティ管理
			ISO/IEC 29100	プライバシーフレームワーク[2]
			ISO/IEC 29134	プライバシー影響評価[2]
	SC 37バイオメトリクス	WG2	ISO/IEC 19784 ISO/IEC 19785	BioAPI 生体認証のAPI
	-	-	ISO/IEC 11889	Trusted Platform Module ※Trusted Computing Groupが公開仕様書を投稿

関連標準規格

情報セキュリティマネジメントシステム ISMS (ISO27000)

分類	番号	内容
用語	ISO/IEC 27000	用語
全般	ISO/IEC 27001	要求事項
ガイドライン	ISO/IEC 27002	ISMSのベストプラクティス
	ISO/IEC 27003	ISMSの要求事項に対するガイダンス
	ISO/IEC 27004	監視、測定、分析、評価の手引
	ISO/IEC 27005	リスクマネジメントのガイドライン
	ISO/IEC 27007	ISMS監査の実施のガイドライン
	ISO/IEC TR 27008	組織の情報セキュリティの管理策のレビュー
要求事項	ISO/IEC 27006	ISMS認証機関への要求事項
	ISO/IEC 27009	ISMSを各セクターに適用した規格の記述方法、様式等
セクター固有のガイドライン	ISO/IEC 27010	セクター間及び組織間コミュニケーションのための情報セキュリティマネジメント
	ISO/IEC 27011	電気通信組織のための指針
	ISO/IEC 27015（**廃止**）	金融サービスのための情報セキュリティマネジメント
	ISO/IEC 27017	クラウドサービスの情報セキュリティ管理策の実践のための規範
	ISO/IEC 27019	エネルギー業界向けプロセス制御システムの情報セキュリティマネジメントに関するガイダンス

分類	番号	内容
セキュリティのガイドライン他	ISO/IEC 27101	サイバーセキュリティの枠組みを策定するためのガイドライン
	ISO/IEC 27102	リスクマネジメントの中でサイバー保険をリスク低減の対策に用いる場合のガイドライン
	ISO/IEC 27103	サイバーセキュリティフレームワークで既存のISO及びIEC規格を活用する方法の手引
その他	ISO/IEC 27013	ISO/IEC 20000-1とISO/IEC 27001の統合実践に関するガイダンス
	ISO/IEC 27014	情報セキュリティのガバナンス
	ISO/IEC 27016	情報資産の保護に対して経済学的な視点を適用し、モデル及び例示の使用を通して情報セキュリティに関する組織の経済性を適用する方法の手引
	ISO/IEC 27021	ISMS専門家の力量に関する要求事項
個別分野	ISO/IEC 27030	IoT
	ISO/IEC 27031	ICTの事業継続への対応
	ISO/IEC 27032	サイバーセキュリティ
	ISO/IEC 27032	ネットワークセキュリティ
	ISO/IEC 27034	アプリケーションセキュリティ
	ISO/IEC 27035	インシデント管理
	ISO/IEC 27036	供給者関係のセキュリティ
	ISO/IEC 2703727041/42/ 43	インシデント調査、デジタル証拠
	ISO/IEC 27039	侵入検知・防御システム(Intrusion Detection and Prevention Systems、IDPS)
	ISO/IEC 27040	ストレージセキュリティ
	ISO/IEC 27050	e-ディスカバリ

NIST: National Institute of Standards and Technology

NIST サイバーセキュリティ・ガイドライン

	略語の意味	内容
SP800シリーズ	Special Publications	コンピュータセキュリティ関係のレポートやガイドライン
FIPS	Federal Information Processing Standards、連邦情報処理標準	米国商務長官の承認を受けてNISTが公布した情報セキュリティ関連の文書
ITL Security Bulletins	-	ITLの会報
NIST IRs	NIST Interagency Reports	NISTの各内部機関がまとめたレポート。CSD Annual Report(年次報告書)など

NIST: National Institute of Standards and Technology

NIST SP800シリーズ

NISTガイドライン番号	タイトル	主な内容
SP800-171	連邦政府外のシステムと組織における管理された非格付け情報の保護	SP800シリーズで保護する情報には、政府の機密情報とされるCI（Classified Information）とそれ以外の重要情報と位置付けられるCUI（Controlled Unclassified Information）の2種類があり、米国では、SP800-171でCUIを管理すると定めている。
SP800-161	システムと組織のためのサイバーセキュリティ・サプライチェーン・リスクマネジメントのガイダンス	調達から販売・供給までの一連のサプライチェーンに存在する業務委託先や関連企業のすべてにおいて、一貫したセキュリティ基準を持つことを定めている　NIST SP800-161の目的は、業務委託先や関連企業におけるセキュリティ対策である。
SP800-53	連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策	米国連邦政府の内部セキュリティ基準を示すガイドライン。

NIST SP800シリーズ

- SP800の基準は多岐にわたる

シリーズNo.（原文発行年月）	タイトル	掲載
SP 800-18 rev.1（2006年02月）	連邦情報システムのためのセキュリティ計画作成ガイド 改訂第1版 Guide for Developing Security Plans for Federal Information Systems	2007年3月
SP 800-30 rev.1（2012年09月）	リスクアセスメントの実施の手引き Guide for Conducting Risk Assessments	2013年2月
SP 800-34（2002年06月）	ITシステムのための緊急時対応計画ガイド Contingency Planning Guide for Information Technology Systems	2005年11月
SP 800-35（2003年10月）	ITセキュリティサービスガイド Guide to Information Technology Security Services	2005年8月
SP 800-37 rev.1（2010年02月）	連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクル Guide for Applying the Ris Information Systems: A S	
SP 800-40 ver.2（2005年11月）	パッチおよび脆弱性管理プロ Creating a Patch and Vuln	
SP 800-45 rev.2（2007年02月）	電子メールのセキュリティに Guidelines on Electronic M	
SP 800-50（2003年10月）	ITセキュリティの意識向上お Building an Information Te Program	
SP 800-52 rev.1（2014年4月）	トランスポート層セキュリテ イドライン Guidelines for the Selectio Security (TLS) Implement	
SP800-53 rev.5（2020年9月）	組織と情報システムのためのセキュリティおよびプライ Security and Privacy Controls for Information Syste	
SP800-53B（2020年10月）	組織と情報システムのための管理策ベースライン Control Baselines for Information Systems and Orga	
SP 800-55 rev.1（2008年07月）	情報セキュリティパフォーマンス測定ガイド Performance Measurement Guide for Information Se	
SP 800-57 Part 1 Rev.5（2020年5月）	鍵管理における推奨事項 第一部：一般事項 Recommendation for Key Management Part 1: General	
SP 800-57 Part 3 Rev.1（2015年1月）	鍵管理における推奨事項 第三部：アプリケーション特有の鍵管理ガイダンス Recommendation for Key Management Part 3: Application-Specific Key Management Guidar	
SP 800-60 Volume I（2004年06月）	第I巻：情報および情報システムのタイプとセキュリティ Guide for Mapping Types of Information and Informa Security Categories	
SP 800-60 Volume II（簡易監修版）（2004年06月）	第II巻：情報および情報システムのタイプとセキュリティ分類のマッピングガイド 付録 Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories	2006年8月
SP 800-61 rev.1（2008年03月）	コンピュータインシデント対応ガイド Computer Security Incident Handling Guide	2009年1月
SP 800-63（2006年04月）	電子的認証に関するガイドライン Electronic Authentication Guideline ※本文書の上位ポリシーOMB M-04-04の翻訳はこちら	2007年8月
SP 800-64 rev.2（2008年10月）	システム開発ライフサイクルにおけるセキュリティの考慮事項 Security Considerations in the System Development Life Cycle	2009年9月
SP 800-70（2005年05月）	IT 製品のためのセキュリティ設定チェックリストプログラム - チェックリスト利用者と開発者のための手引き Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers	2007年3月
SP 800-73 rev.1（2005年04月）	個人識別情報の検証インタフェース Interfaces for Personal Identity Verification	2006年10月
SP 800-76-1（2007年01月）	個人識別情報の検証における生体認証データ仕様（改訂版） Biometric Data Specification for Personal Identity Verification（rev.1）	2009年10月
SP 800-81（2006年05月）	セキュアなドメインネームシステム（DNS）の配備ガイド Secure Domain Name System （DNS） Deployment Guide	2009年9月
SP 800-82 rev.2（2015年5月）	産業制御システム(ICS)セキュリティ Guide to Industrial Control Systems (ICS) Security	2016年3月
SP 800-83（2005年11月）	マルウェアによるインシデントの防止と対応のためのガイド Guide to Malware Incident Prevention and Handling	2008年9月
SP 800-84（2006年09月）	IT計画およびI ド Guide to Test, Capabilities	
SP 800-86（2006年08月）	インシデント対 Guide to Integ	
SP 800-88 rev.1（2014年12月）	媒体のデータ抹 Guidelines for	
SP 800-92（2006年09月）	コンピュータセ Guide to Com	
SP 800-94（2007年02月）	侵入検知および Guide to Intru	
SP 800-130（2013年08月）	暗号鍵管理システム設計のフレームワーク A Framework for Designing Cryptographic Key Management Systems	2020年7月
SP 800-144（2011年12月）	パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン Guidelines on Security and Privacy in Public Cloud Computing	2014年3月
SP 800-145（2011年09月）	NISTによるクラウドコンピューティングの定義 The NIST Definition of Cloud Computing	2011年12月
SP 800-146（2012年05月）	クラウドコンピューティングの概要と推奨事項 Cloud Computing Synopsis and Recommendations	2012年8月
SP 800-171 rev.2（2020年2月）	非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	2021年2月
SP800-172（2021年2月）	管理対象非機密情報を保護するための拡張セキュリティ要件: NIST SP 800-171の補足 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	2021年8月
SP 800-175A（2016年8月）	米国連邦政府での暗号標準利用のためのガイドライン：指令、命令、及び方針 Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies	2021年5月
SP 800-175B rev.1（2020年3月）	米国連邦政府での暗号標準利用のためのガイドライン：暗号メカニズム Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms	2021年5月
SP800-190 rev.1（2017年9月）	アプリケーションコンテナセキュリティガイド Application Container Security Guide	2020年9月
SP800-207（2020年8月）	ゼロトラスト・アーキテクチャ Zero Trust Architecture	2020年12月

NIST: National Institute of Standards and Technology

関連標準規格

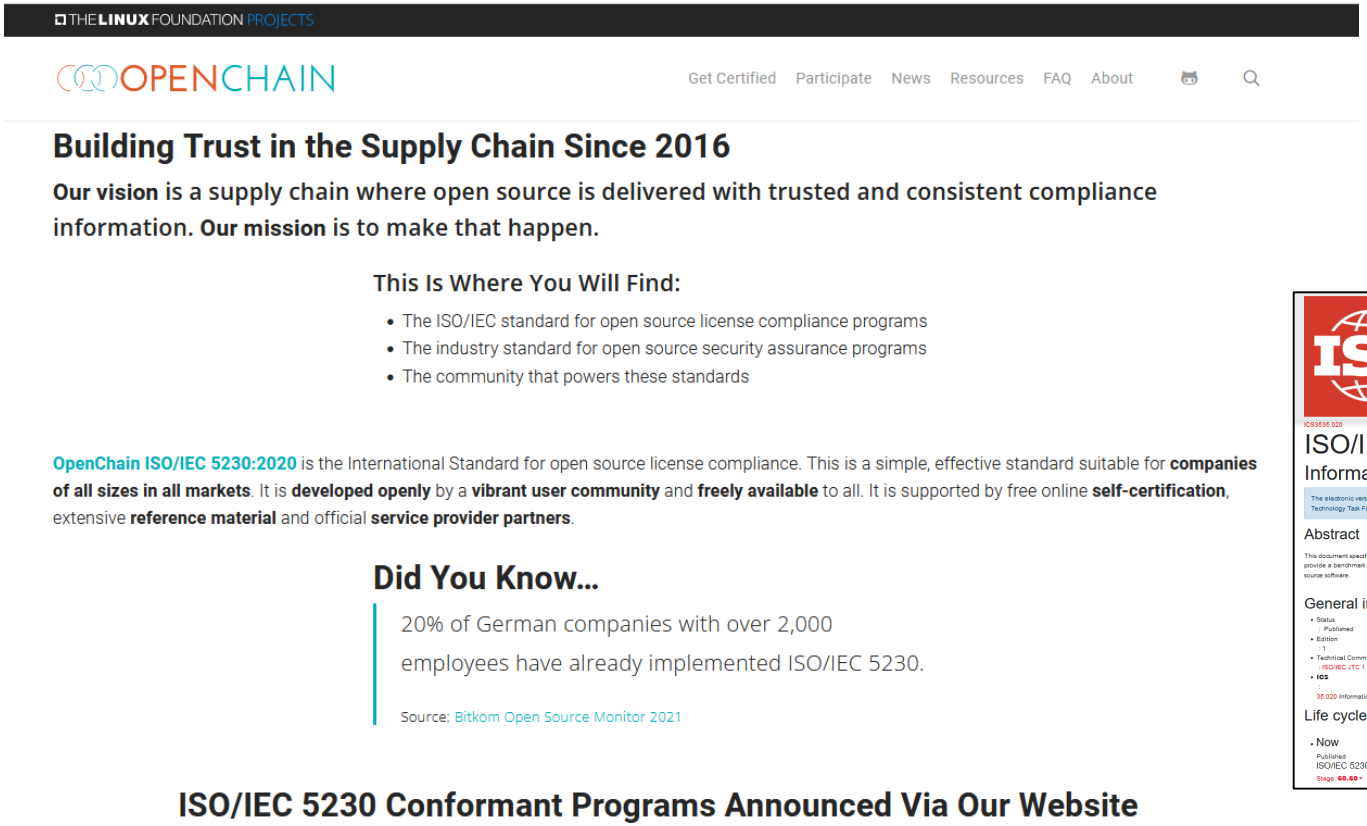
IEC 62443（産業用制御システムセキュリティ）

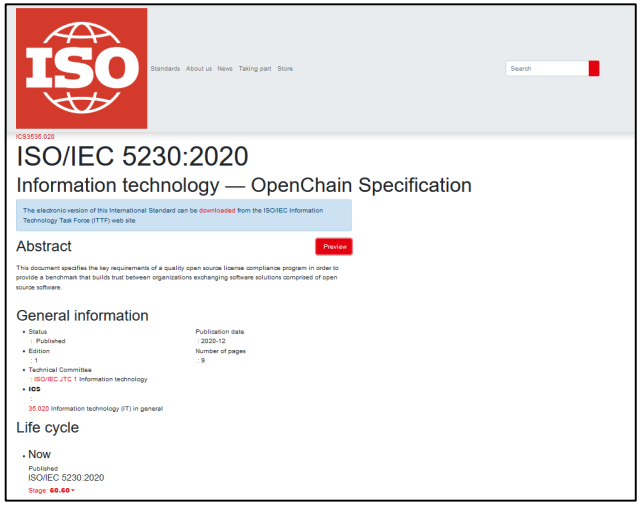
区分	主な対象者	番号	名称	認証	
全般	共通事項	62443-1-1	Terminology, Concepts, and models		
		62443-1-2	Master glossary of terms and abbreviation		
		62443-1-3	System security compliance metrics		
		62443-1-4	IACS security lifecycle and use-case		
セキュリティプログラム	事業の要件	62443-2-1	IACS security management system - Requirement	CSMS	
		62443-2-2	Implementation guidance for an iacs security management system		
		62443-2-3	Patch management in the IACS environment		
	事業者とインテグレータの共通の要件	62443-2-4	Security program requirement for IACS service providers		
システム	インテグレータの要件	62433-3-1	Security technologies for IACS		
		62433-3-2	Security Risk Assessment and system design		
	インテグレータと製品開発者の共通の要件	62433-3-3	System security requirement and security levels		SSA
部品	製造開発者の要件	62433-4-1	Secure Product development lifecycle requrement	EDSA	
		62433-4-2	Technical security requirement for IACS component		

	制御システムセキュリティ	ITシステムセキュリティ
組織/ポリシー/手順のセキュリティ	IEC62443	ISO27001
システムセキュリティ規準		
コンポーネント製品セキュリティ規準		

OpenChain ISO/IEC 5230

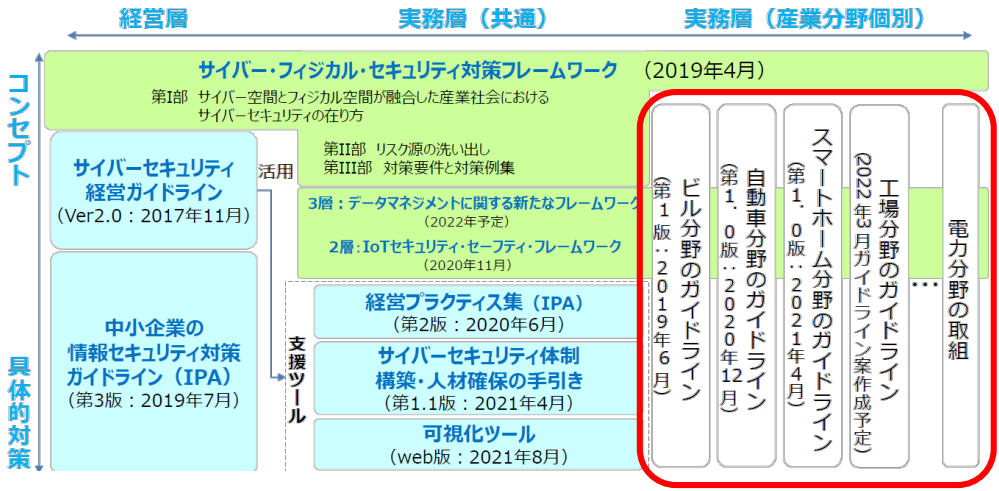
- OSSのライセンスコンプライアンスプログラムを組織が構築するための指針を整備しているプロジェクト。
- OSSコンプライアンスのために組織が満たすべき要件を示す仕様書、チェックリスト、トレーニング資料や参考資料、認証プログラムなどで構成される。ISO標準化もされている。
- SBOMの仕様であるSPDX、SPDX-Liteも標準化している。





業界ガイドライン

- サイバーセキュリティのガイドラインは業界ごとに多岐に渡る



出典:：経産省資料　電力分野におけるサイバーセキュリティ について 資料６
2019年8月29日 資源エネルギー庁
https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/020_06_00.pdf

出典: 経済産業省 第8回産業サイバーセキュリティ研究会 ワーキンググループ2
（経営・人材・国際）資料3　2022年3月23日
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/008_03_00.pdf