

サプライチェーン強靱化におけるデータ連携の仕組みに関するガイドライン（車載半導体 関連）（0.1 beta版）

パブリックコメント

番号	対象文書	提出された意見	ご意見に対する回答
1	本文	<p>総論</p> <p>本ガイドラインは、自動車産業における車載半導体のサプライチェーン強靱化という喫緊の課題に対し、ODS-RAMに基づくデータスペース設計を具体化した意欲的な取り組みであり、業務フロー・ビジネスアーキテクチャの整理は実務に即した高い水準にあると評価いたします。</p> <p>一方で、本ガイドラインが扱うデータ（生産地、プロセスノード、ウエハサイズ、キャパシティ情報、EOL計画等）は各半導体メーカーにとって極めて機密性の高い競争情報であり、データスペースへの参加インセンティブはデータ保護の信頼性に直結します。以下、主としてセキュリティアーキテクチャの観点から意見を述べます。</p> <p>意見1：データ主権の暗号的担保に関する設計指針の追加を求める 該当箇所 -本文 5.2.1 半導体情報提供機能における開示制御の仕組み（p.48） -附属書D #5.4 データ暗号化（伝送データの暗号化） -附属書D #5.7 改ざん防止（指標・例ともに未記載）</p> <p>意見 現行の開示制御設計は、ALL（全開示）/ RESTRICTED（限定開示）のアクセス制御により、データスペース運営事業者のプラットフォーム機能としてデータ主権を実現する構成となっています。しかし、この設計ではデータスペース運営事業者自身（およびその基盤提供者）が全データの平文にアクセスし得る状態が前提となり、以下のリスクが残存します。</p> <ul style="list-style-type: none"> ・運営事業者の内部不正またはインフラ侵害時の全データ露出 ・政府・規制当局による強制的なデータ開示要求への対応困難（特に海外拠点や国際連携時） ・半導体メーカーにとって「プラットフォームを信頼せよ」という要求が参加障壁となる可能性 <p>附属書D #5.4では「伝送データの暗号化」のみが記載されていますが、蓄積時の暗号化（encryption at rest）について、データ提供者が鍵の主権を保持する設計（data owner key sovereignty）の指針が必要です。具体的には、TPM（Trusted Platform Module）やTEE（Trusted Execution Environment）を活用し、データスペース運営事業者であっても平文データにアクセスできない構成を、将来的な設計目標として明記することを提案します。</p> <p>また、附属書D #5.7「改ざん防止」の指標・例が空欄となっていますが、EOL情報やキャパシティ情報の完全性は有事対応の根幹であり、暗号学的な完全性検証（例：データ提供時のデジタル署名、immutable audit trail）の設計指針を記載すべきと考えます。</p>	<p>3.1「トレードシークレット要件」において「データ連携の仕組みに関するガイドラインの手引きサプライチェーン共通編 1.0版」の2.3を参照しています。参照先においてデータスペース運営事業者が全データの平文にアクセスし得る状態を前提としておりません。また、附属書Dは非機能要件例を提供し、実サービスにおいては適切に設計されるものと考えております。</p> <p>なお、附属書D #5.7「改ざん防止」の指標・例が空欄との指摘ですが、データスペース運営事業者としては当該非機能を検討する必要があります。</p>
2	本文	<p>意見2：秘密計算（Privacy-Preserving Computation）の選択肢に関する記載を求める 該当箇所 -本文 第4章 ビジネスアーキテクチャ全般 -本文 第5章 5.1 データスペースの機能配置図 -附属書C データ項目（安定調達・BCP、新陳代謝促進）</p> <p>意見 本ガイドラインの業務フローでは、半導体メーカーが自社データをデータスペースに登録し、OEM・部品メーカーが当該データを参照する「1:N開示」モデルが基本です。この構成は個別参照には有効ですが、今後想定される以下のユースケースへの拡張に課題があります。</p> <ul style="list-style-type: none"> ・業界全体の供給リスクの統計的把握（例：特定プロセスノードの全メーカー合算キャパシティ） ・有事における代替サプライヤーの探索（競合他社のキャパシティを個社単位で開示せずに実現） ・複数OEMの需要集計と半導体メーカーの供給能力のマッチング <p>これらは、個社データを平文で運営者に預託する現行モデルでは実現が困難であり、秘密計算技術（準同型暗号、秘密分散、マルチパーティ計算等）の適用が有効です。とりわけ、Multi-Key Fully Homomorphic Encryption（MKFHE）は、各社が独自の鍵で暗号化したまま集計・比較演算を行い、復号には関係者全員の合意を要する方式であり、本ガイドラインが掲げる「トレードシークレットの保護」と「データ連携による業界共通便益」の両立に適しています。</p> <p>0.2版以降の検討項目として、「秘密計算技術の適用可能性の検討」を明記し、特に附属書Cに記載される数値データ（キャパシティ、台数、製品数等）を対象とした集計処理への適用を視野に入れることを提案します。</p> <p>なお、本意見はDADCが推進するウラノス・エコシステムにおけるScope3 CO₂データ連携でも同種の課題が議論されており、領域横断での設計原則の共通化が効率的と考えます。</p>	<p>御提案の秘密計算技術について、目的に沿った手段であると認められる場合にはガイドラインの更新時に採用されうると考えております。</p>
3	本文	<p>意見3：耐量子暗号（Post-Quantum Cryptography）への対応指針を求める 該当箇所 -附属書D #5.4 データ暗号化 -本文 1.3 ガイドラインの位置づけ（ロードマップ：v1.0版が2028年度予定）</p> <p>意見 本ガイドラインのロードマップでは、v1.0版が2028年度に予定されており、ライフサイクル期間は5年（附属書D #3.8）とされています。すなわち、本データスペースは2033年頃まで運用される想定です。</p> <p>NIST PQ標準（ML-KEM、ML-DSA等）が2024年に確定しており、暗号学的コミュニティでは2030年代にCRQC（Cryptanalytically Relevant Quantum Computer）が実用化される可能性が議論されています。本データスペースが扱う半導体サプライチェーン情報は、数年経過後も競争上の価値を持つため、harvest-now-decrypt-later攻撃の対象となり得ます。</p> <p>v1.0版策定時までに、伝送暗号化および蓄積暗号化においてPQCアルゴリズム（ML-KEM-768等）への移行ロードマップを含めることを提案します。0.2版の段階では、非機能要件としてPQC対応を検討事項に明記するだけでも、参加事業者の設計判断に寄与すると考えます。</p>	<p>「2033年ごろまで運用される想定」との御意見ですが、本ガイドラインは運用期間を定めておりません。耐量子暗号については目的に沿った手段であると認められる場合にはガイドラインの更新時に採用されうると考えております。</p>

サプライチェーン強靱化におけるデータ連携の仕組みに関するガイドライン（車載半導体 関連）（0.1 beta版）

パブリックコメント

番号	対象文書	提出された意見	ご意見に対する回答
4	本文	<p>意見4：国際相互運用性に関する補足 該当箇所 -本文 5.1 データスペースの機能配置図（ODS-RAM参照） 意見 欧州ではCatena-Xが自動車サプライチェーンのデータスペースとして稼働しており、半導体分野においてもSemi-conductor Supply Chain Data Spaceの議論が進んでいます。Catena-XはGaia-X / IDSA（International Data Spaces Association）のアーキテクチャに基づき、DID（Decentralized Identifiers） / VC（Verifiable Credentials）をアイデンティティレイヤーに採用しています。 本ガイドラインのp.13にて「将来的には汎用半導体及び自動車業界以外への適用拡大を考慮」と記載されていますが、国際的なデータスペースとの相互運用を視野に入れる場合、アイデンティティレイヤー（L3）におけるDID/VCとの整合性を早期に検討することが望ましいと考えます。 これは、意見1で述べたデータ主権の暗号的担保とも密接に関連します。DID/VCを基盤としたアイデンティティ管理は、プラットフォーム運営事業者に依存しない分散的な信頼モデルを実現し、国際連携時のトラスト構築に寄与します。 まとめ 本ガイドラインの業務設計・アーキテクチャ設計は高く評価するものであり、上記の意見は0.1 beta版の段階でこれらの論点を明示的に検討組上に載せることを求めるものです。特に意見1（暗号的データ主権）および意見2（秘密計算）は、半導体メーカーの参加インセンティブに直結する要素であり、データスペースの社会実装の成否を左右し得ると考えます。 以上</p>	<p>DID/VCについては現時点の業務要件にありません。他データスペースとの連携手段の1つとして重要なポイントであると認識しております。</p>
5	本文	<p>本文p.4 「サプライチェーン強靱化」というスコープだが、p.4の位置付けにも現れているように自動車産業における自動車向け半導体のみをスコープとしている。自動車以外の最終製品や、自動車向け以外の一般半導体といった汎用的な半導体のデータ連携にも活用できそうに見受けられるため、将来を見据えてガイドラインとしてのスコープを自動車以外に広く構えたいうえで、今回のユースケースが車載向けであるという建付けにしたほうが良いのではないか。</p>	<p>御指摘を受け、1.1節に汎用的な活用可能性についての記述のスライドを追加しました。</p>
6	本文	<p>本文p.8 データプラットフォームをDPFと表記しているが、公益デジタルプラットフォームもDPFと表記がされる。データプラットフォームとデジタルプラットフォームの違いは何か。用語集等で補足説明を行った方がよい。 https://www.ipa.go.jp/digital/dx/dpf-nintei.html</p>	<p>御指摘の通り、誤解を招かないよう「半導体データプラットフォーム（半導体DPF）」と表現を改めました。</p>
7	本文	<p>本文p.37 ビジネスアーキテクチャでは、データ提供者はデータスペースから価値提供を受けている図となっている。一方、p.42の実現できるサービスを見ると、データ提供者が便益を受けられるようには見えない。この場合の「価値提供」は何を指すのか。データ提供者がDPFにデータを提供するメリットやインセンティブを明確に記すべきである。</p>	<p>例えばデータ提供者はデータスペースを利用することで様々な情報の個別問合せコストを効率化できるというメリットがあります。データ利用者は複数社のデータを半導体DPFの統一されたUI・データ形式で活用できます。御指摘を踏まえ、p.42「半導体データプラットフォームで実現できるサービス」のスライドのレイアウトを改善しました。</p>
8	本文	<p>本文p.48 開示制御の対象となる粒度はデータ項目の粒度か、それとも全体か。 例えば付属書Cにおける新陳代謝促進の情報全体または「部品別参考情報」のデータ項目のみを、特定のOEMにのみ開示するという制御は可能か。開示制御の粒度を明確にすべきである。</p>	<p>p.48に記載の通り「誰に」「何を」開示するかを指定できるとしており、本ガイドラインは製品情報の全体若しくは部分のいずれを指定するようには記載していません。社会実装時に必要な粒度を調整できることを念頭に置いています。御質問のような「部品別参考情報」のみを開示する機能を否定していません。</p>
9	付属書C：データ項目	<p>付属書C p.3 データ項目「代替部品」はどのレベルで記載するのか。自社の代替部品か、他社の代替部品を含むのか。また、EOLに対する後継部品がある場合、それは代替部品となるのか。用語や表現、説明を含めて、丁寧な説明が必要である。加えて、データ提供者にとって便益があるデータ項目とすべきである。</p>	<p>代替部品については半導体メーカーが独自に決定するものと考えております。</p>
10	付属書D：非機能要件	<p>付属書D p.4 非機能要件#2.3の20,000製品程度は妥当か。汎用品でも数千～数万点ほどあるケースがある。バリエーションや時間軸で見ても十分にスケールするか？もう少し柔軟性が必要ではないかと考える。算定根拠を示せば良いのではないかと。</p>	<p>ユースケースの実現にあたりステークホルダによる確認を経て現在の表現としておりますが、スケールアウトに言及しているものの御指摘の現実に対応するには表現を改善する必要があると考え、 「20,000製品以上」と改めました。</p>
11	本文	<p>1.P4 ・「スコープ」に示される企業間契約によるトラスト形成が「データスペースとの利用契約によるトラスト形成」で置き換えることが可能である根拠の記載が欲しい。</p>	<p>本ガイドラインの前提文書である「データ連携の仕組みに関するガイドラインの手引きサプライチェーン共通編 1.0版」の2.4節で取引基本契約をトラストの根拠の例として挙げています。本ガイドラインでは取引基本契約のない各者間によるデータ連携を想定していますので、データスペースとの利用契約をトラストの根拠の例としています。置き換え可能であるという表現は誤解を招きますので当該項目の文章を改めました。</p>

サプライチェーン強靱化におけるデータ連携の仕組みに関するガイドライン（車載半導体 関連）（0.1 beta版）

パブリックコメント

番号	対象文書	提出された意見	ご意見に対する回答
12	本文	<p>2.P37</p> <p>・「データベースは一定程度の中立性が担保された事業者が運営し、すべてのステークホルダにとって公平な費用と便益が持続可能な形で設定され、すべてのステークホルダが各自の役割を認識し合意が形成されるようにすること。」</p> <p>上記が充足されていることが確認できる項目及び基準の記載が欲しい。</p> <p>また、システムの機能・非機能要件だけでなく、システムの運用・管理要件についても同様の記載が欲しい。</p> <p>・データベース運営事業者間（データベース運営事業者とそれとは別のデータベース運営事業者の間）のデータ連携に関する取決めについての記載及びその取決めが充足されていることが確認できる項目及び基準の記載が欲しい。</p>	<p>それぞれに回答いたします。</p> <p>・当該記述はサービス企画・運営時にステークホルダに開かれた意見照会の場合が提供されていることと、サービスの事業継続性があることで確認されると考えています。なお、本ガイドラインはデータ連携の仕組みとして機能・非機能の要件を扱っており、運用・管理については一部の要件に触れていますが、サービスレベルにも関係する領域であることから記述しておりません。</p> <p>・相互運用性は本ガイドラインの前提文書である「データ連携の仕組みに関するガイドラインの手引き サプライチェーン共通編 1.0版」の2.5節で扱っており、プロトコルの標準化を挙げています。この一例としては認証・認可の仕組みをOpen Data Space（ODS）を参照することや、API仕様を提供可能とすることが挙げられます。</p>
13	本文	<p>3.P38</p> <p>・「データベース運営事業者」の役割「アプリケーション事業者のアプリケーションを認証する。」</p> <p>上記が充足されていることが確認できる項目及び基準の記載が欲しい。</p> <p>・「データベース運営事業者」の役割「オンボーディングプロセスを提供」</p> <p>上記、オンボーディングプロセスを明確にして欲しい。</p> <p>・「データベース運営事業者」の役割「安全性と信頼性を持続的に維持しながら、データベースを管理・運営する。」</p> <p>上記が充足されていることが確認できる項目及び基準の記載が欲しい。</p>	<p>それぞれに回答いたします。</p> <p>・アプリケーションの認証については、データベースとの技術的な接続機能の検証や、利用者へのサポート体制の整備状況等、様々な項目が考えられます。一律に基準として提示することは難しいです。</p> <p>・オンボーディングプロセスはデータベース運営事業者の裁量によるため、一律に基準として提示することは難しいです。プロセスの一部の例として、参加希望者の真正性を一般の企業間取引の開始時等に用いられる手段で証明することが挙げられます。</p> <p>・安全性や信頼性等については公益デジタルプラットフォーム運営事業者認定制度において申請時に運営事業者が説明する内容であり、安全性や信頼性の捉え方を示した上で、管理・運用できる体制やプロセスを提示することが求められると考えています。</p>
14	本文	<p>4.P40</p> <p>・「川下から川上へデータ提供を依頼する際は、相手方を公正に扱うための配慮事項を整理し、提示することが望ましい。」</p> <p>上記、必須ではないのか？</p> <p>必須であれば、「指針の範囲」「適切な管理体制」「同じ部品」「無理のないスケジュール」「必要に応じて」「努めること」「関連する法案」等の明示が欲しい。</p>	<p>半導体データプラットフォームにおいては、データを提供する川上企業はデータを利用する川下企業の依頼がなくともデータを開示・提供することが通常のケースと考えています。その上で川下企業が川上企業へデータ提供を依頼する場合は当該配慮事項を提示することが必須要件との御指摘であると理解し、要件として必須と改めました。なお、各者の業務環境にも関係するために「指針の範囲」等の具体化は避け、現状の表現のままとしております。</p>
15	本文	<p>5.P47</p> <p>・「半導体データプラットフォームに対して機能概要を詳細化したものとして機能要件を示す。」</p> <p>上記が充足されていることが確認できるようにするために、正常・準正常・異常も含めた確認項目と基準の記載が欲しい。また、必須機能とオプション機能の区別が欲しい。</p>	<p>本ガイドラインでは機能要件を示していますが、実装様態までは示していないため、確認項目と基準を記載しておりません。なお、半導体データプラットフォームとして、ここに列挙されている機能要件はすべて必須です。</p>
16	本文	<p>6.P56</p> <p>・「〔附属書D：非機能要件〕に例示する。」</p> <p>このガイドラインがシステムに求める非機能要件の基準（必須又はオプション及びそのレベル）の記載が欲しい。</p>	<p>非機能要件については附属書Dで指標を例示しており、データベース運営事業者が附属書Dのすべての要件を検討するよう指示するものですが、P56の記載に不足があるため記述を追加しました。</p>
17	附属書C：データ項目	<p>データ項目の必須・オプションの区別の記載が欲しい。</p> <p>また、それぞれの設定が「例」となっているが、相互運用を行うためには解釈に齟齬がないようにするための定義が必要と考える。</p>	<p>附属書Cが扱う部品補足情報、新陳代謝促進、安定調達・BCPの各データはデータ提供者の裁量により半導体DPFに登録されるデータであるため、実態としてはオプション扱いになります。</p>