一般社団法人
伝送データセキュリティ評議会（SDC）

設立趣意書（第五版）

データ伝送におけるセキュリティの世界標準と
標準に適合した極小複合チップ及びシステムを創出することで
社会に貢献いたします。

使命と目標

評議会の使命

データ伝送におけるセキュリティの世界標準と
標準に適合した極小複合チップ及びシステムを創出することで
社会に貢献いたします。

本評議会のミッションは伝送データの連続性と真正性を保証する通信プロトコル（ハッシュチェーン）とチップにおける固有識別（PCA：Physical Cyber Authentication）を統合した「伝送データセキュリティ」を実現する専用チップ及び専用チップを活用したトータルシステムの創出とそれを応用するための世界標準を創出することにあります。

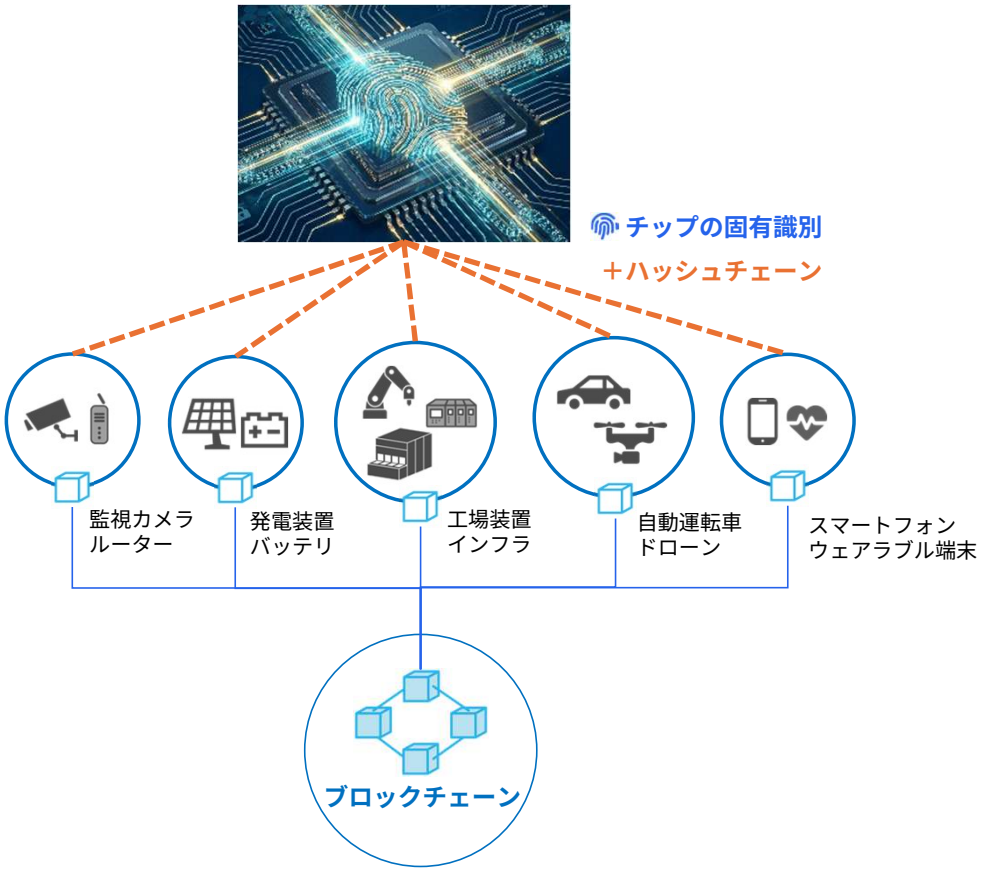
新たな世界標準（ISO）を創出するにはその技術を共有できる複数の企業が連携しノウハウを集約し多方面からの研究が必要となります、その結果においてあらゆる産業で安心してデータ伝送が行える強固なインフラが構築できると確信しています。

対象市場と目標売上（ISO創出後 2029.7〜）

デジタルパスポート市場 **3,396億円**
（VPN、防衛、バッテリ、医療、…等）
AI市場 **4,388億円**
（V2X、監視、生体認証、…等）
データ付加価値市場 **3,095億円**
（脱炭素、P2P取引、PHR、…等）

※用語
VPN：Virtual Private Network
V2X：Vehicle to Everything
P2P：Peer to Peer
PHR：Personal Health Record

合計予測市場　**約1兆円**
シェア10%獲得　目標売上　**1,000億円**　知財ライセンス収益　**100億円**



※標準適合チップ潜在市場（対象市場）：各市場規模の1%で算出

Confidential

目次

改訂履歴

版数	改訂日	主要な改訂内容
第一版	2026年3月5日	評議会設立に伴う初版発行。
第二版	2026年3月23日	「映像データの真正性欠如」に関する課題を追加。これに伴い技術体系・プロダクト群を再編。会員特典における割引価格体系を具体化。
第三版	2026年3月26日	「スマートモビリティにおける経済安全保障」に関する課題を追加。自動運転、自律制御、V2X（Vehicle-to-Everything）、スマートキー等を含むコネクテッド・エコシステムへの対応に伴い、技術参照アーキテクチャおよび標準適合プロダクト群を拡充。
第四版	2026年4月10日	「5か年ロードマップ」および、各重点セクター（デジタルパスポート、AI、データ付加価値化）における具体的な「市場予測データ」と「活用事例（知財戦略を含む）」を拡充・再編。一般会員を正会員と名称変更。
第五版	2026年4月20日	「リアルタイム常時接続社会における通信プロトコル自体の構造的課題」を追加、物理層認証によるログインレスな社会像の提示。あわせて、資料全体の権利保護および利用上の注意を明文化するため「免責事項（Disclaimer）」の項目を新設。

Confidential

評議会設立の目的

伝送データの信頼基盤の構築

※NDAA (National Defense Authorization Act)　米・国防権限法
※CRA (Cyber Resilience Act)　欧・サイバーレジリエンス法

現代のグローバル市場では、国際規制（NDAA/CRA等）への対応が不可欠となっています。製品の安全性や来歴を客観的に証明できないものは**市場から排除されるという厳しい時代**が到来しています。

他方ではAIや自律制御の普及により意思決定を左右する「データ」の信頼性が重要視されています。しかし従来の対策は端末やサーバーの保護が中心であり**伝送経路でのデータ改ざん（データ汚染）という大きな死角**が残っています。特に次世代の社会インフラである「スマートモビリティ」の領域では、センサデータや映像データ、ならびに自動運転・自律制御における走行コマンドやスマートキーの認証情報の汚染が、車両の暴走や重大な事故に直結します。これらを防ぐため、データの発生源からAIを含めた目的地まで一貫して伝送データの信頼性・安全性を守る技術基盤の確立が、企業の生存戦略において急務となっています。

本評議会のミッションは伝送データの連続性と真正性を保証する通信プロトコル（ハッシュチェーン）とチップにおける固有識別（PCA：Physical Cyber Authentication）を統合した**「伝送データセキュリティ」を実現する専用チップ及び専用チップを活用したトータルシステムの創出とそれを応用するための世界標準を創出する**ことにあります。

新たな世界標準（ISO）を創出するにはその技術を共有できる複数の企業が連携しノウハウを集約し多方面からの研究が必要となります、その結果においてあらゆる産業で安心してデータ伝送が行える強固なインフラが構築できると確信しています。

🏳 2026年2月17日、本評議会を設立いたしました。
産官学の連携により**データ伝送セキュリティ標準**を確立致します。

伝送データセキュリティ

デバイス固有の物理的特性を起点に、真正・機密・完全・可用性の4要素をEnd-to-Endで一気通貫に満たすデータ伝送セキュリティ技術

今すぐ解決すべき６つの課題

課題① 市場からの非セキュリティ製品の排除

証明不能な「来歴・固有識別・完全性」が招く市場排除の危機

米国国防権限法（NDAA）や欧州サイバーレジリエンス法（CRA）等は、**ハードウェアの真正性証明**を実質的に義務付けています。

国際法規制（NDAA/CRA等）が求める「真正性（Authenticity）」とは、以下の3要素が物理層から技術的に裏付けられた状態を指します。

来歴（Provenance）の証明不能 → 部材の真正性

禁止部材混入の有無を客観的に証明できないためサプライチェーン全体のリスクとなる。

固有識別（Identity）の脆弱性 → 機器の真正性

ソフトウェア認証だけではデバイスの「なりすまし」や「取り違え」を物理的に防げない。

完全性（Integrity）の欠如

データが改ざんされていないことを物理層から証明できない限り、信頼性は担保されない。

これらを担保できない製品は、グローバル市場から
「Untrusted」として強制排除
されるリスクに直面しています。

今対策を打たなければ、グローバルサプライチェーンから切り離されるリスクがあります

課題② 工場の稼働停止とデータの信頼性欠如

ネットワーク内部の「通信の汚染」と「物理的侵入」リスク

境界防御を突破した後の「**内部ネットワークにおける不正な通信行為**」や、「**悪意あるデバイスの物理的な継ぎ足し**（物理的侵入）」に対し、現在の伝送プロトコルは物理層に基づいた検証手段（証跡）を持っていません。

未認証機器の接続リスク

物理的な固有識別が不十分で、不正デバイスによる偽命令の混入を防げません。

通信経路でのデータ改ざん

物理的根拠に基づく署名等がなく経路上の改ざんを検知不能なため不正操作を許容します。

来歴不明なデータの混入

客観的な来歴の証拠がなくデータの真偽を判定不能で、事後検証が困難です。

稼働停止とデータ改ざんは、製造業の「信用」を根底から破壊します

課題③ 映像データの真正性欠如

監視・検査システムへの「映像注入」の脅威

無人工場や自律稼働ロボットにおいて映像は単なる記録ではなくAIが「判断し、動く」ための絶対的な根拠です。**入力情報の「物理的根拠」**が失われることで、自動化の前提となる安全性が根本から崩壊します

通信路への直接的な「偽映像」の割り込み

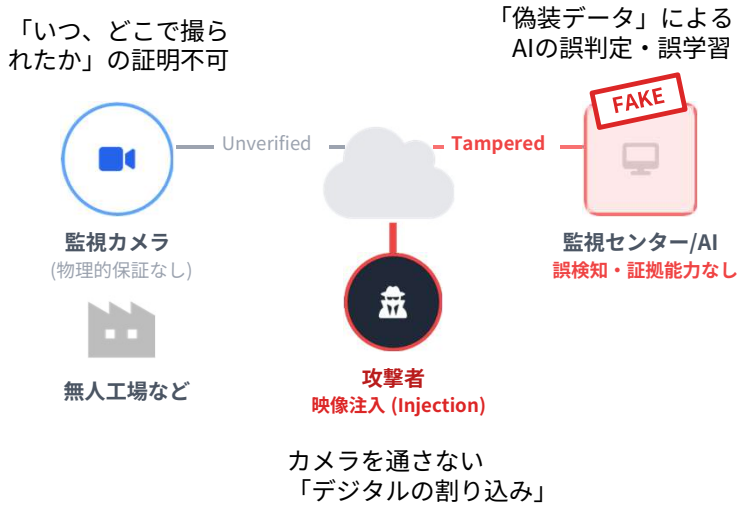
通信経路にAI生成映像（ディープフェイク）を直接割り込ませ、監視網の無力化や物理的な不法侵入を許容します。

証跡としての「撮影事実」の証明不能

1フレームごとの物理的紐付けがないため、映像の中抜きや過去映像のループ再生といった改ざんを検知できません。

AIを欺く「視覚的データ汚染」

人間には判別不能な微細な書き換えにより、AIの検知・認証アルゴリズムを意図的に誤作動させます。



映像データの『真正性欠如』は自律制御の前提を根底から覆し、システムを制御不能なリスクへと変貌させます。

課題④ AI・自律制御の信頼性

「汚染されたデータ」によるAIの暴走と事故リスク

自律制御システムにおいて、入力データはAIが「判断し、行動する」ための絶対的な根拠です。しかし、現在のAIシステムは**「正しい発信元から、改ざんされずに届いたデータ」であることを物理層から検証する「信頼の起点（Root of Trust）」を欠いています。**

データポイズニング（Data Poisoning）

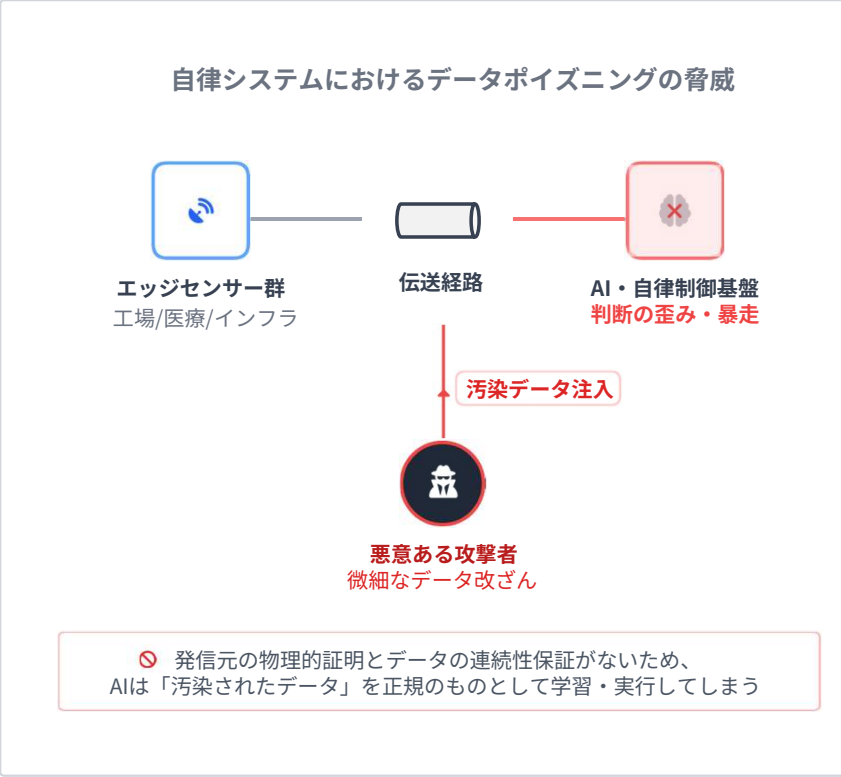
悪意ある「汚染データ」をAIが取り込むことで、意図的な誤認識や暴走を誘発されます。

無線通信の脆弱性

有線と異なり、信号到達圏内であれば物理的侵入なしに外部から遠隔攻撃（なりすまし・改ざん）が可能です。

物理的な「信頼の起点」の欠如

正しい発信元から改ざんされずに届いたことを物理層から保証する仕組みが不可欠。



物理的な「信頼の起点（Root of Trust）」から続く改ざん不能なデータ保証が不可欠です。

課題⑤スマートモビリティにおける安全保障

車両・ドローン・生体情報を結ぶネットワークに潜む、なりすましとサイレント改ざんの脅威

現行の通信プロトコルでは「送信元が物理的に本物か」を検証できず、デバイスのなりすましや、通信路での改ざんを物理層に直結した仕組みで遮断する手段がありません。このことが経済安全保障上の重大なリスクとなっています。

制御権の奪取（車両・ドローン・ヒューマノイド）

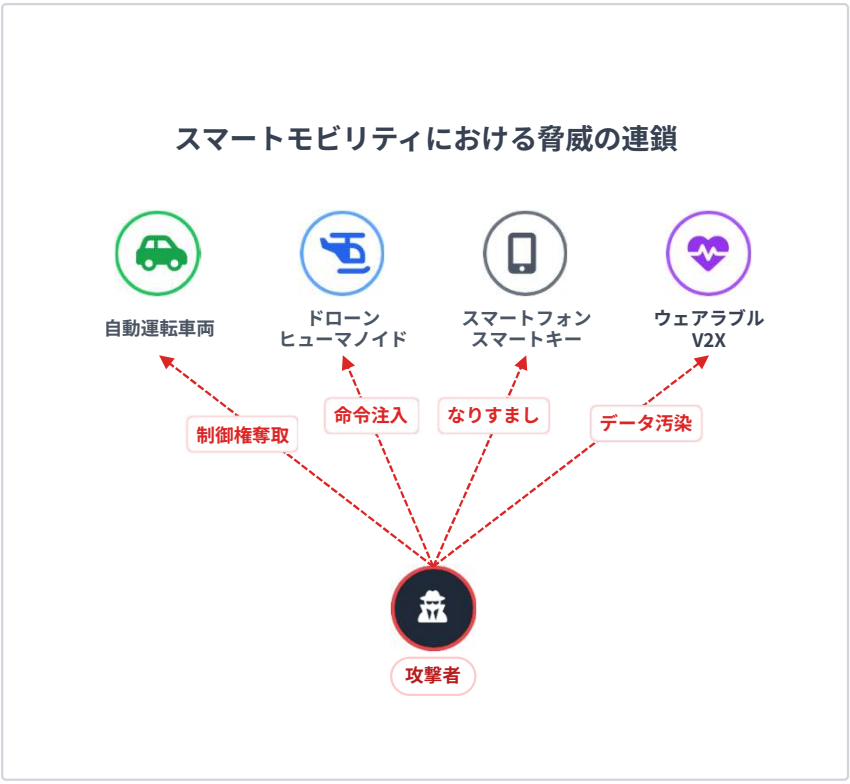
操作コマンドにハッシュチェーン（連続性保証）がない場合、第三者による命令注入や通信の中継（リレーアタック）を防げず、物理的な暴走や墜落、盗難を許容します。

デジタル接点のなりすまし（スマートフォン・スマートキー）

PCA（チップにおける固有識別）がないソフトウェア依存の認証ではスマートフォンを介したデジタルキーの偽装やなりすましを物理的に根絶できず、基幹インフラへの不正侵入を招きます。

バイタル・センサーデータの汚染（ウェアラブル・V2X）

スマートウォッチから送られるドライバーの健康情報や路側センサーのデータが改ざんされた場合、AIが誤った判断を下し、緊急停止の失敗や人命に関わる事故を誘発します。



物理層から連続する『伝送データの真正性』こそが、命を預かるモビリティ社会の絶対的な安全基盤です。

課題⑥リアルタイム常時接続社会における通信プロトコル自体の構造的課題

データの「アイデンティティ」と「正当性」を即時かつ継続的に証明できない構造的限界（TCP/IPの限界）

リアルタイム常時接続社会では、流れるデータの真正性を立ち止まることなく検証し続ける必要があります。しかし、接続維持に特化した既存体系は検証をソフトウェア層の処理に依存しており、速度と安全性を両立できない構造的課題を抱えています。

伝送効率の限界とデータ自体の真正性保証

パケットごとのヘッダ解析負荷が物理層の性能を阻害しており、高速・低遅延な伝送を実現するためには伝送データ自体に真正性を判断する要素を組み込むことが必須となります。

認証プロセスに伴う自律制御の阻害

ソフトウェア層でのセッション確立や証明書確認の手順がデバイス間の即時連携を妨げており、通信ごとのログインや複雑な接続手順を不要にするハードウェア主導の自動認証への転換が求められます。

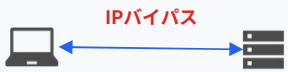
個体識別とデータの乖離による秘匿性の欠如

既存プロトコルは通信路を保護するのみでデータの物理的出自を証明できません。物理層の固有識別とデータを直結させ、正当な権利を持つ者だけが受信データを閲覧できる仕組みが不可欠です。

ポストIPに向けた世界的潮流

SCION (次世代インターネット)

送信側が信頼できる経路を直接指定し、IPの脆弱性を克服する新アーキテクチャ。



IOWN APN (オールフォトニクス)

電気処理を排し光のまま伝送することで、物理限界に近い低遅延を実現するインフラ。

V2X Sidelink (車両間直結)

IP層を介さず直接通信し、ミリ秒単位で状況を同期するモビリティ専用規格。

AIセマンティック通信 (AI専用)

生データではなく、AIが理解する「意味（ベクトル）」のみを最小単位で送り届ける次世代方式。

物理層から自動的に真正性が証明される仕組みこそが次世代インフラの本命です。

理想的な世界標準の新体系

Confidential

伝送データセキュリティの理想とする体系

伝送データセキュリティ標準では、ISO/IEC 27000のセキュリティ基本概念（Confidentiality/機密性・Integrity/完全性・Availability/可用性・Authenticity/真正性）を基盤とし、これを次世代の脅威を見据えて拡張します。「PQC（耐量子計算機暗号）」や時系列の「連続性」、さらに物理層のRoot of Trustとなる「チップ固有識別」と「ハードウェア・レジリエンス」を融合。エッジデバイスから通信プロトコル階層までを一気通貫で保護し、データの正しさと確実なシステム稼働を担保する新たな国際標準を確立します。

Confidentiality

未来の脅威でも「漏れない」か？

機密性＋PQC（耐量子計算機暗号）

量子計算機による将来的な暗号解読リスクに対し、PQC（耐量子計算機暗号）を実装することで、長期間にわたりデータの秘匿性を担保し続けることが不可欠です。

Integrity

データが「途切れず無傷」か？

完全性＋連続性

単発のデータ改ざん防止にとどまらず、制御コマンドや映像ストリームの順序・欠落を含めた時系列の連続性を保証することで、リプレイ攻撃（過去データの再利用）や巧妙なデータ注入を確実に遮断します。

Authenticity

機器が「物理的に本物」か？

真正性＋物理認証（チップ固有識別）

ソフトウェア上の鍵に依存せず、チップ固有の物理特性を認証の根拠とすることで、デバイスのなりすましを物理層から排除し、センサー値から映像、V2X（Vehicle-to-Everything）における制御コマンドに至るあらゆる入力情報の「発生源」の真正性を直接証明します。

Availability

攻撃下でも「止まらせない」か？

可用性＋ハードウェア・レジリエンス（強靭性）

攻撃時の過負荷で正当な信号を選別できず停止する課題に対し、ハードウェア層の自律的な制御により、本物の信号のみを選別・優先処理する強靭性の確立が不可欠です。

伝送データセキュリティの確立

物理層から通信路までを一気通貫で保護し、確実な稼働を担保する仕組みを提供

世界標準創出へ

Confidential

ISO新規規格 提案概要

規格名称：ハードウェアを起点とした伝送データの完全性およびデバイス真正性のための参照アーキテクチャ

1. 提案の背景

実社会のインフラがデジタルと密接に連携し自動制御されるシステムの普及に伴い、汎用OSや既存の通信の脆弱性を突いたデータ改ざんが深刻なリスクとなっている。特にAIの判断材料や自動制御のコマンドにおいて、ソフトウェア層の侵害に左右されない「信頼の起点（Root of Trust）」が不可欠である。本提案は、ハードウェアを基盤とし、データの生成から終端まで一貫して真正性を証明する参照アーキテクチャを規定する。

2. 適用範囲

エッジデバイス（センサ・アクチュエータ）から、ゲートウェイ、クラウドに至るエンド・ツー・エンドのデータ伝送過程。産業制御システム（ICS）やAI外観検査等の高度な判断を伴うシステム、ならびに自動運転・ドローン等の「自律移動体」とその運行管制、V2X通信、およびスマートキー等のアクセス管理システムなど、高度な安全性とリアルタイム性が要求されるミッションクリティカル・システムに適用する 。

3. 主要な要求事項

3.1 ハードウェアに基づく個体識別:　**PUF（物理複製困難関数）等の物理的特性から派生した一意の識別子を用い**、デバイスの全ライフサイクルにわたり、ソフトウェアの改ざんから独立した真正性（Authenticity）を確立すること。

3.2 実行プロセスの完全性保護:　**データの真正性確認および非改ざん性の証明に用いる演算処理は、メインOSにおける他のプロセスや外部からの干渉を受けない、独立したリソースまたは保護された実行属性を用いて実行**されること。

3.3 継続的な完全性の連鎖:　3.1の識別子に基づき、「暗号学的ハッシュ連鎖」や「メッセージ認証コードによる連鎖（MAC Chaining）」等の手法を用いて、**データ生成から受信に至るまでの連続的な完全性を証明すること**。受信側は3.2で定義された保護環境内でこの動的な連鎖検証を行い、ストリームデータの非改ざん性をリアルタイムで保証すること。

3.4 ハードウェアに依拠した自律的レジリエンス:　**検証に失敗したデータや不正トラフィックを、上位アプリケーション層に到達する前に破棄するフィルタリング機能を備える**こと。攻撃下においても、攻撃時においても、ハードウェアの優先度制御機能（割り込み制御等）を直接活用することで、数ms以内の決定論的な処理を維持すること。

4. 期待される効果

本アーキテクチャは、特定ベンダーの実装（専用ASIC、セキュアエレメント等）に依存せず、データそのものの信頼性を客観的に評価する基準を提供する。これにより、サプライチェーン全体のリスクを低減し、自動化システムの安全な社会実装と経済安全保障の強化に寄与する。

標準に適合する技術と製品

革新技術が融合した伝送データセキュリティベーシックモデル（コア技術）

(株)シーズ 代表取締役会長兼CEO 伊東久雄氏

ハッシュチェーン

機密性＋PQC
次世代の脅威を見据えた強固な暗号化で伝送データを保護

完全性＋連続性
改ざん防止に加え、正しい順序で通信されている「連続性」を保証

真正性
デバイス認証した端末からのデータであることを保証するが、物理的な確証は持たない

可用性＋強靭性
過負荷攻撃下でも正当な命令を識別・優先し、制御の継続性を死守する

＋

台湾 国立陽明交通大学 教授 渡辺浩志氏

チップ固有識別（PCA）

真正性＋物理認証
複製不可能なチップの固有識別（PCA）により、物理的なデバイスの真正性（本物である確証）を付与

→

伝送データセキュリティ基盤
（グローバル・モデル）

物理層直結のRoot of Trustにより、ハードウェアと伝送データの真正性を一体で担保する独自開発・世界初のセキュリティ基盤

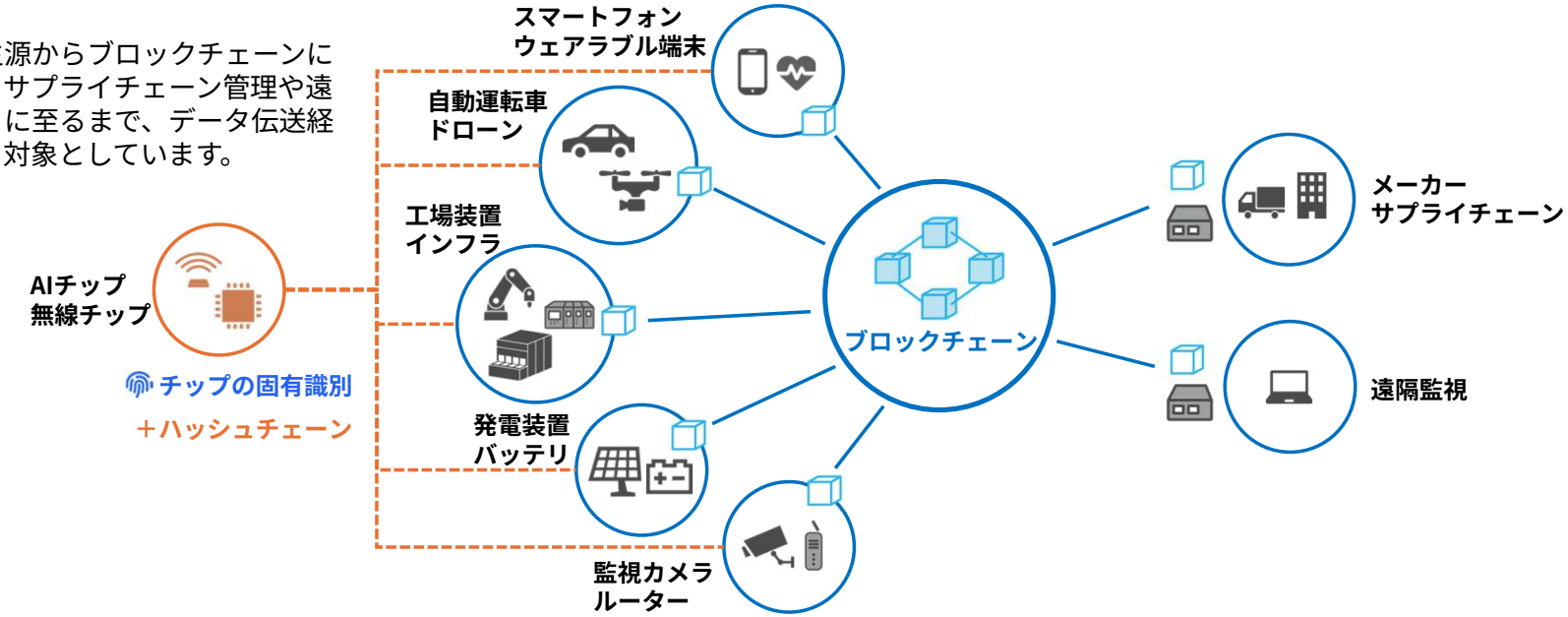
- PQCで将来の解読を防ぎ秘匿を担保
- PCA物理認証でなりすましを根絶
- ハッシュ連鎖で順序保証と攻撃遮断
- 攻撃下でも正当な命令を優先し死守

IT黎明期から各種制御システムやOSの基幹技術に深く携わり日本唯一の日本語版Linuxを開発した(株)シーズ 代表取締役会長兼CEO 伊東久雄氏は、伝送データの真正性・完全性を追求する中で、デバイス自体の物理的真正性の証明という課題に直面しました。一方、デバイス物理の権威である台湾 国立陽明交通大学 教授 渡辺浩志氏は10年以上にわたりPCAの研究を続けてきました、しかし実証する組み込み技術が実用化への大きな障壁となっていました。この二人が出会うことにより伊東氏の持つOS・プロトコル技術により渡辺氏のPCA技術は実現可能な具体的なシステムとして世に誕生しました。両者の技術が融合したことで通信ごとに物理層から真正性を証明し続ける「究極の次世代伝送データセキュリティモデル」が完成しました。この技術をグローバルな『信頼の標準』として確立し、物理層から連続する伝送データの真正性証明を世界へ普及させることで、次世代の経済安全保障を主導し、これらの技術を核とした強固な伝送データセキュリティの実現により世界で最も安全なスマートモビリティ基盤を構築します。

Confidential

本評議会が実現させる伝送データセキュリティ

本標準は多様なデータの発生源からブロックチェーンによる「客観的な証跡記録」、サプライチェーン管理や遠隔監視等の「高度な利活用」に至るまで、データ伝送経路の全行程においての保護を対象としています。



01

物理層　PUF / なりすまし防止

チップ固有の物理特性（PUF等）でデバイスを厳格に識別。複製不可能なIDを信頼の根源とし、なりすましを物理レベルで遮断します。

02

伝送路　リアルタイム検知

データをハッシュチェーン技術で連結し、生成から伝送完了までを保護。通信経路上でのリアルタイムな改ざん検知を実施します。

03

記録層　客観的証跡の確立

物理層から届く信頼の連鎖を永続的に記録・証明するブロックチェーン。データ証跡を提供する。

04

活用層　安全なデータ活用

信頼の連鎖により真正性を保証。エンドユーザー（オフィス／社内PC）は出所と内容が証明されたデータを安全に活用できます。

Confidential

標準適合プロダクト群

物理層 & 伝送層

ハッシュチェーンチップ ＋ PCA

センサ・映像・スマートキー認証等の伝送データを検証 。不正介入やリレーアタックを物理層から検証して遮断し、真正性を保証する 。

ブロックチェーンチップ ＋ PCA

センサ数値や映像フレーム等の記録データに対し、ブロックチェーンに記録して証跡を生成 。改ざん不能な信頼性を永続的に担保する

自律分散AIセル ＋ PCA

センサ・映像等のAI入力データへのポイズニングを排除 。真正なデータによるAI推論を支援し、自律システムの安全を担保する 。

スクランブルメモリ ＋ PCA

チップ固有IDとハッシュチェーンを用いて、制御信号や画像データをメモリ階層で直接保護するセキュアメモリ 。

記録層

ブロックチェーン

物理層から届く信頼の連鎖を永続的に記録・証明する分散型台帳。

監査証跡としての客観性を担保。

活用層

ブロックチェーン ゲートウェイ ＋ PCA

ブロックチェーンノードを実装した中継機で、クラウドへ安全に接続する。

ブロックチェーン トランスフォーマー＋PCA

PCに接続されたブロックチェーンノード実装の小型端末。

専用Linux OS（チップ用、組み込みボード用、クラウドサーバー用）

チップ、IoT、クラウドの各層に最適化された専用OS。ハードウェアの性能を最大限に引き出し、デバイス固有の識別や高度なセキュリティ機能を安定して動作させます。

専用SDK（ハッシュチェーン、ブロックチェーン、スクランブルメモリ）

コア技術を活用するための開発キット。チップ固有値の呼び出しやハッシュチェーン生成・検証、ブロックチェーンへの記録・取得をサポートし、信頼性の高いシステム実装を容易にします。

評議会概要

評議会概要

法人概要

法人名

一般社団法人 伝送データセキュリティ評議会
Security of Data Transfer Council （SDC）

設立日

2026年2月17日

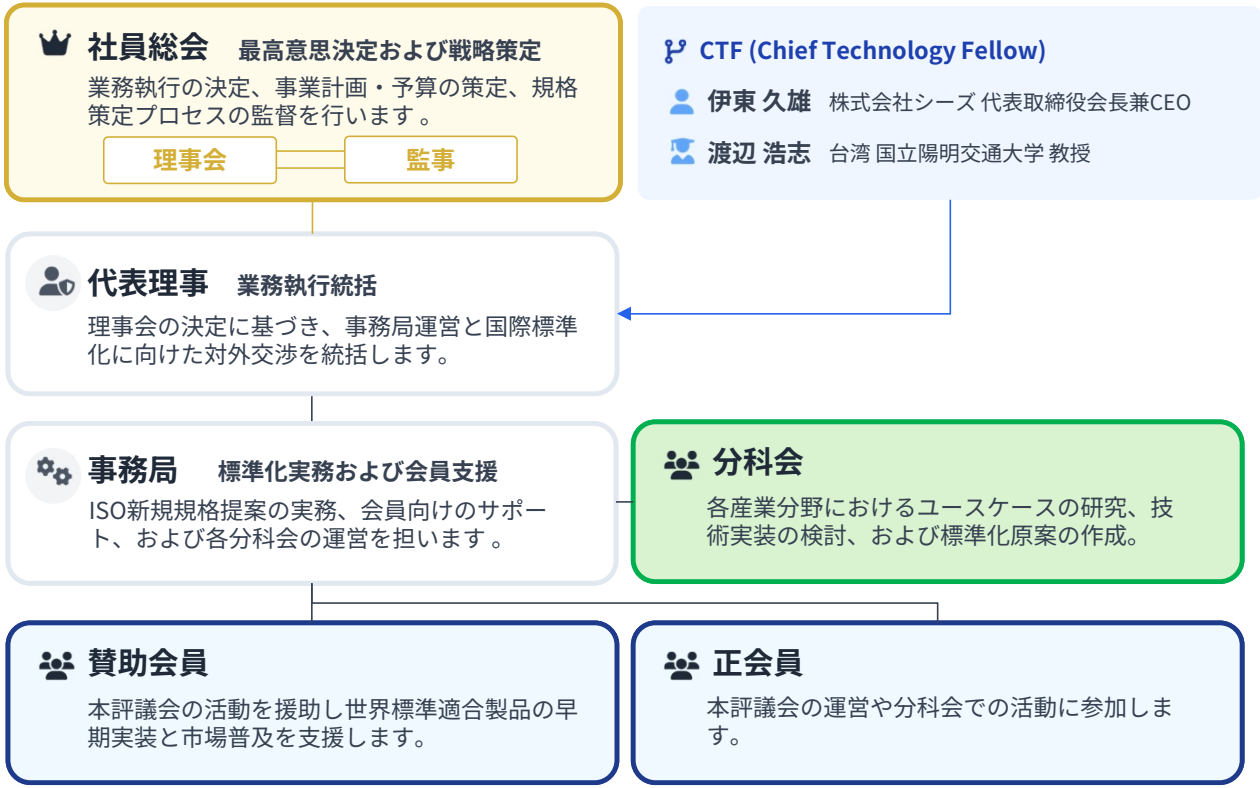
代表理事

後藤 勝由　当法人専任

事業目的

- 伝送データセキュリティの世界標準（ISO等）の創出
- 標準に適合した専用チップ及びトータルシステムの創出
- 強固なインフラ構築による産業社会への貢献

ガバナンス体制



活動予算

活動予算（発足から5年間）

技術開発費　約3億円

（新規チップを開発する場合、約28億円）

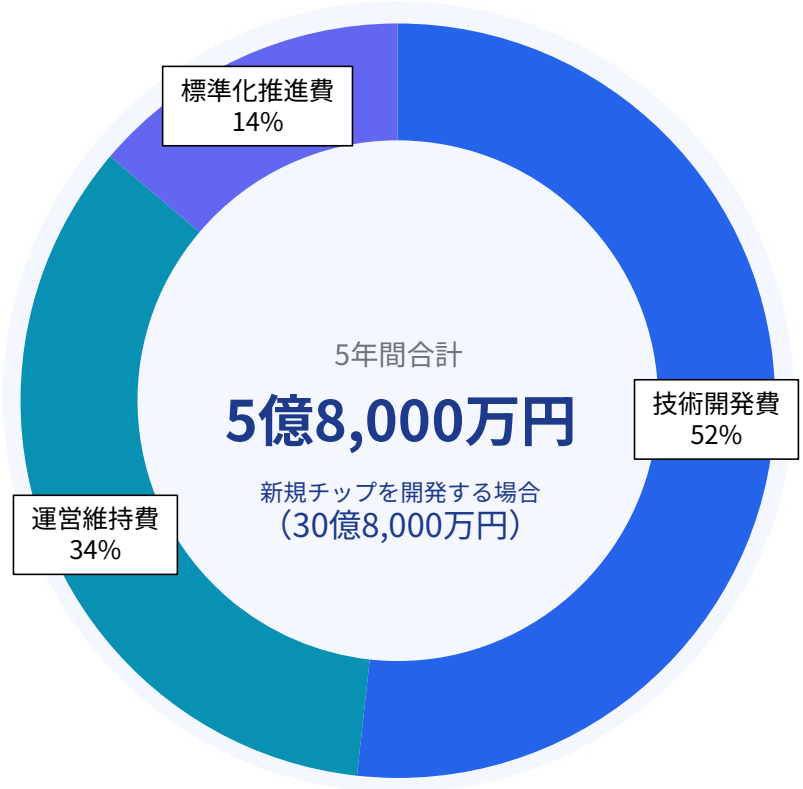
策定するセキュリティ世界標準に準拠した世界初の極小複合チップとSDK及びクラウド構築・運用費用。

運営維持費　約2億円

事務局・拠点運営に加え、セミナーや広告による戦略的な情報発信、国際交渉や現場支援を確実に担保するグローバル渉外費用。

標準化推進費　約8,000万円

専門コンサルタントを活用したISO/IEC規格の策定実務と、発行後の維持・連携費用。技術を世界のルールとして定着させ、市場への普及を牽引する費用。



6年目以降は主に運営維持費のみとなります。（一年間＝約3,000万円）
正会員の入会金＋年会費で賄えるとみています。

本評議会は、革新的技術開発においては公的予算を戦略的に活用しつつ、事務局運営や国際標準化活動などの基盤業務については、会費収入による自立した運営体制を構築します 。

Confidential

5か年ロードマップ

開発 標準化 特典 PoC

2026.7 - 2027.6	2027.7 - 2028.6	2028.7 - 2029.6	2029.7 - 2030.6	2030.7 - 2031.6
第1期 **仕様策定**	**第2期** **SDK先行配布** **専用チップ試作**	**第3期** **専用モジュール完成** **社会実装PoC**	**第4期** **ISO規格創出** **グローバル展開**	**第5期** **IEC規格創出**
開発 専用チップの回路設計	**開発** 専用チップの試作製造	**開発** 専用モジュール(量産型)完成	**標準化** **ISO国際規格発行（2029.7）と普及活動**	**標準化** **IEC規格発行 （2030.7）と普及活動** **インフラ要件化**（半導体等の製造工場、ドローン、ロボット、自動運転車等）
標準化 ISO標準原案(ドラフト)提出	**開発** SDK v1.0 先行配布 専用LinuxのPoC	**PoC** ドローン/自動運転等でPoC	**開発** 量産販売/ライセンス供与開始	**開発** 次世代版(v2.0)要件定義
会員特典 WG参画		**標準化** 実証エビデンスをISOへ提出	**会員特典** 標準取得コンサル開始	

収益① 会費（賛助会員費、正会員費）

賛助会員

会員区分	賛助会費 (一括)	計画数 (5年間)
プラチナ	3,300万円(税込)	7社
ゴールド	1,100万円(税込)	10社
シルバー	550万円(税込)	10社

正会員

会員区分	入会金	年会費	計画数 (5年間)
正会員	55万円(税込)	5.5万円(税込)	100社以上

特典

	プラチナ 賛助会員	ゴールド 賛助会員	シルバー 賛助会員	正会員
運営参画（理事選出）	○ （1名）	―	―	―
ISO WGへの招待	○ （優先）	○ （優先）	○	―
技術特許ライセンス	○ （※特別価格）	○ （※割引価格）	○ （※割引価格）	○
開発チップ・SDKの購入	○ （※特別価格）	○ （※割引価格）	○ （※割引価格）	○ （※割引価格）
PoC技術サポート	○ （無償）	○ （※割引価格）	○ （※割引価格）	○ （※割引価格）
標準取得コンサルティング実施権	○	―	―	―
セミナー（Web含む）への参加	○	○	○	○
各種イベントへの参加	○	○	○	○
最新情報の閲覧（会員サイト）	○	○	○	○

※特別価格：　プラチナ賛助会員50%OFF
※割引価格：　ゴールド賛助会員30%OFF、シルバー賛助会員20%OFF、正会員10%OFF

収益② 公的予算

政府動向

政策背景

政府も金融にブロックチェーンを活用することについて検討していることを公開しており今後浸透していく可能性があります。

予算動向

経済安全保障推進法に基づき、基幹インフラの防御や先端技術の育成を目的としたサイバーセキュリティ関連予算が、過去最大の規模で投入されています。

評議会の意義

政府系の予算を得るためにも一社では力不足であり複数の企業が集まることで予算を獲得する可能性が高くなります。

ターゲットとする主な公的予算・国家プロジェクト（例）

＜執行機関＞ 制度・事業名	公募 時期	予算規模 （1件あたり）	プロジェクトの概要と SDCの申請内容案
＜防衛装備庁＞ **安全保障技術研究推進制度**	4～5月	最大5億～ 10億円	安全保障分野における将来の装備品に適用可能な革新的基礎技術の育成 → PCAの「物理的複製困難性」とハッシュチェーンによる「命令改ざん防止」を用いた基礎研究
＜NEDO＞ **ポスト5G基盤強化** 先端半導体製造技術開発	3～4月	数十億～ 数百億円 規模	次世代AIチップ等の国内設計・製造基盤の確保による産業競争力の強化 → エンジンレスPUF及びハッシュチェーン制御部分をASIC（専用チップ）化し、ハードウェア階層に実装
＜NEDO＞ **ポスト5G基盤強化** データエコシステムの構築 （GENIAC）	3月～	数十億円 規模	国産生成AI開発に不可欠な高品質データセットおよび計算資源の整備 →物理に直結したPCAとハッシュチェーンの統合により、データの発生源からAI推論エンジンまでの真正性を一気通貫で保証。物理階層からの証跡により、AIへの入力データが『汚染（ポイズニング）』されていないことを証明
＜NEDO＞ **ウラノス・エコシステム実現のための データ連携実証**	3～4月	数億～ 十数億円 規模	業界の垣根を越えたセキュアなデータ共有基盤「ウラノス」の構築・社会実証 → サプライチェーン全体のデータ伝送において、PCAとハッシュチェーンによるEnd-to-Endの真正性を保証
＜経済産業省＞ **グリーンイノベーション基金** スマートモビリティ社会の構築	4～6月	数億円 規模	自動運転やL4ドローン等の社会実装を通じた移動の脱炭素化と高度化 → 自動運転やV2X通信における「なりすまし」を、セッション層で動的に防ぐSRoT（セッション・ルートオブトラスト）を構築
＜経済産業省＞ **標準化推進事業費補助金** （国際ルール形成型）	随時	数千万円 規模	日本発の革新技術を国際標準（ISO）化し、世界市場での主導権を確保 → PCAとハッシュチェーンを組み合わせた日本発の参照アーキテクチャを、ISO等の国際標準として確立

> **政府は経済安全保障に基づき、ポスト5G基盤強化や重要技術育成プログラム等に過去最大級の予算を投入中です。これら大規模プロジェクトへの参画は一社では極めて困難ですが、本評議会での連携により獲得が現実的となります。**

対象市場と活用事例

市場予測・収益ビジョン（標準適合チップ市場規模）

算出ロジック

装置・システム全体市場：　評議会趣意書に記載の各産業分野の合算値
標準適合チップ潜在市場：　全体市場の1%と定義
目標売上：　潜在市場における獲得シェア10%と定義

ターゲット市場予測
3つのカテゴリ別に市場規模を分析

カテゴリ	装置・システム合計市場	標準適合チップ潜在市場	目標売上	シェア
デジタルパスポート市場 VPN・防衛・電池・医療等	33兆9,585 億円	**3,396 億円**	340 億円	**10%**
AI市場 V2X・監視・生体認証等	43兆8,810 億円	**4,388 億円**	439 億円	**10%**
データ付加価値化市場 脱炭素・P2P取引・PHR等	30兆9,450 億円	**3,095 億円**	309 億円	**10%**
合計予測 3カテゴリ合算	**108兆7,845 億円**	**1兆878 億円**	**1,088 億円**	**10%**

長期収益ビジョン

チップ関連総売上目標
1,000億円
ターゲット市場シェア10%獲得

知財ライセンス収益目標
100億円
標準周辺特許のライセンス（売上の10%）

知財・ライセンス戦略の3本柱

標準周辺特許の確立と秘匿
基本技術はオープン化（標準化）し、実装・最適化の周辺特許で収益化。

高収益ライセンスモデル
自社チップ販売に加え、他社SoCやモジュールへのIP提供による安定的なロイヤリティ収益を確立

国際取引の「物理的通行証」化
特許網により、経済安全保障に不可欠な「物理層の信頼」を提供

1．デジタルパスポート市場

経済安保と国際相互承認の「絶対条件」

ネットワーク・インフラの「物理的ゼロトラスト」とサプライチェーン強靭化

1. 絶対的課題：非関税障壁（DPP/電池規則）への物理認証と「製造証明」の義務化

欧州のデジタル製品パスポート（DPP）に加え、2026年本格適用・2027年完全施行の欧州CRA（サイバーレジリエンス法）への対応。

ルーター、VPNゲートウェイ、車載通信ユニットに**「ハードウェアベースの信頼の起点」**を要求。

真正性を証明できない製品の市場排除リスク。特に化学品・半導体材料の上流工程における「不透明な産地・品質」の解消。

2. 国策との連動：経済安全保障推進法および「ウラノス」の物理レイヤー

経産省**「ウラノス・エコシステム」**における物理層の信頼の起点としての専用チップの機能。

特定重要物資のサプライチェーンを物理的認証で担保し、欧州Catena-X等との相互承認を得る。

不測事態における「説明責任」を全うするための最強の証拠。

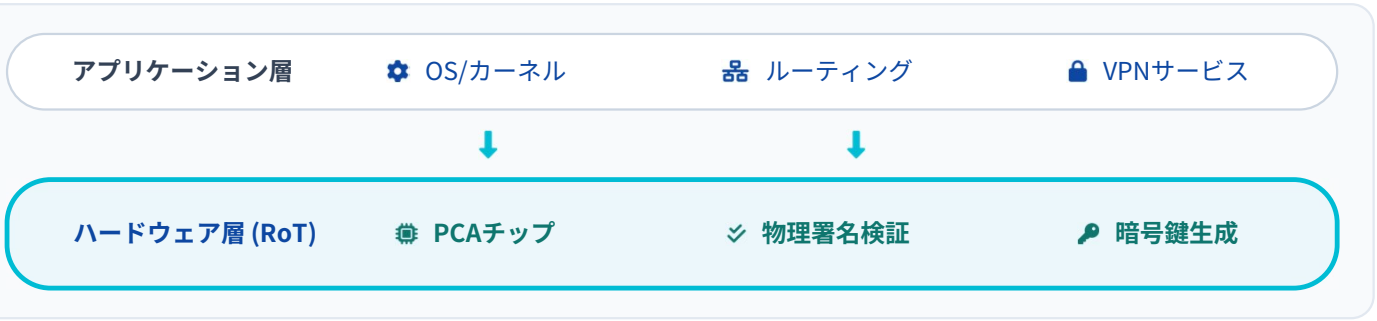
日欧ブリッジ：物理的ゼロトラスト

1－1．ルーター・VPN・通信モジュール

課題と解決策

インフラを支えるルーターやVPN機器において、アップデートを装った**不正なファームウェアの混入**（サプライチェーン攻撃）が深刻な脅威となっています。**欧州CRA法（2024年12月施行・2027年完全適用）**にも対応する物理的な固有識別検証とハッシュチェーンを導入することで、改ざんされた伝送データを完全に遮断します。

活用事例：セキュアルーター内部アーキテクチャ



改ざん防止アーキテクチャ

OSやファームウェアが起動する前に、ハードウェア層のPCAモジュールが署名を検証し、改ざんされた伝送データを遮断します。

市場規模データ　VPN（仮想プライベートネットワーク）

世界市場(2026)	日本市場	米国市場
860.2億ドル	6,340億円	210億ドル

ソース

タイトル: Virtual Private Network (VPN) Global Market Report 2026
発行元: The Business Research Company (Research and Markets)
URL: https://www.researchandmarkets.com/reports/5767522/virtual-private-network-vpn-market-report

１－２．防衛装備品・特定重要物資

課題と解決策

経済安全保障推進法および**米国NDAA**に基づき、政府調達の条件として「製造証明」と不正部品の排除が必須となっています。
サプライチェーン攻撃の脅威に対し、上流工程からの物理的な来歴管理を実装し、Catena-X DPP等(2026年運用開始)と連携することでデータ改ざんを防ぎます。

サプライチェーン攻撃
不正部品
データ改ざん

対策 →

物理トレーサビリティ
ハッシュチェーン来歴管理

保証 →

真正性証明
NDAA調達要件
クリア

活用事例： 半導体サプライチェーンの物理的来歴管理

市場規模データ　Defense Cyber Security Market

世界市場(2026)	日本市場	米国市場
203.5億ドル	**1,580億円**	**98.7億ドル**

ソース
タイトル: Defense Cyber Security Market Size & Analysis, 2026-2033
発行元: Coherent Market Insights
URL: https://www.coherentmarketinsights.com/market-insight/defense-cyber-security-market-5087

1－3．バッテリパスポート

課題と解決策

欧州電池規則に対応し、採掘からリサイクルまでのデータを**物理的に紐付け**。
真正性を物理証明できない電池はEU域内流通不可となります。
各セルに専用チップを搭載し、セルIDと充放電データに物理署名を付与します。

トレーサビリティ欠如
データの断絶
偽装リスク

法規制要件 →

DPP準拠
デジタル製品パスポート

物理証明 →

EU市場流通
市場アクセス確保

活用事例： EV電池の階層構造と物理署名

セル
専用チップ内蔵

モジュール
複数セル統合

パック
筐体化

BMS
状態監視・署名

クラウドDPP
データ真正性確保

階層的トレーサビリティ

セルに組み込まれた専用チップが、組み立て後のモジュール・パック全体の状態データに物理署名を付与し、クラウドへ安全に送信します。

市場規模データ　デジタル製品パスポート（DPP）

世界市場(2026)	EU市場	日本市場
3.8億ドル	2.1億ドル	30億円

ソース

タイトル: Digital Product Passport (DPP) Market Size, Share, Analysis | 2035
発行元: Dimension Market Research
URL: https://dimensionmarketresearch.com/report/digital-product-passport-dpp-market/

１－４．医療機器・ウェアラブル医療端末

課題と解決策

遠隔医療やオンライン治験において、**バイタルデータの改ざんやなりすまし**が患者の生命に関わる重大なリスクとなります。
デバイスに専用チップを組み込み、データ発生源での物理署名により真正性を証明し、安全な医療データ連携を実現します。

データ偽装・改ざん
命に関わるリスク

バイタル送信 →

Chip固有識別＋Hashchain
発生源での真正性付与

安全伝送 →

医療データベース
信頼できる診断へ

活用事例： 医療データセキュア伝送経路図

STEP 1
ウェアラブル医療端末
PCAによる
チップ固有識別

BLE
Bluetooth →

STEP 2
スマホゲートウェイ
ハッシュチェーン検証

5G
インターネット →

STEP 3
医療用クラウド
真正性
検証・保存

エンドツーエンド保護
測定した生データはウェアラブル内で物理的に署名され、中継デバイス（スマホ）を経由しても改ざん不可能なまま医療従事者に届きます。

市場規模データ　医療機器セキュリティ

世界市場(2026)	日本市場	米国市場
83億ドル	820億円	34.5億ドル

ソース
タイトル: Medical Device Security Market Size, Share & Growth Analysis [2034]
発行元: Fortune Business Insights（Research and Marketsでも販売）
URL: https://www.fortunebusinessinsights.com/medical-device-security-market-115040

１－５．状態監視(Condition Monitoring)

課題と解決策

保守や中古市場での価値算定において、**稼働ログの改ざん**が大きなリスクとなっています。
製造装置や重機のセンサーから出力されるデータを物理レベルで固有識別することで、真正性証明を付帯した改ざん不可能な保守履歴を実現し、資産価値を担保します。

改ざんされたログ
資産価値の低下・偽装

チップ起因の固有識別 →

Chip固有識別＋Hashchain
送信元を識別

価値担保 →

信頼された監査証跡
真正性証明済み

活用事例：セキュア状態監視システム図

製造装置・重機
センサーデータ計測

稼働ログ →

物理層保護
専用チップ
真正性・連続性保証

セキュア送信 →

クラウド保管基盤
時系列保存
監査証跡提供

真正性の証明
データ発生源での物理封印によりクラウド上での改ざん不可能性を保証。中古評価や保険算定の信頼できる根拠となります。

市場規模データ　状態監視システム

世界市場	日本市場	米国市場
42億ドル	520億円	16.8億ドル

ソース
タイトル: Machine Condition Monitoring Market Size, Share & Trends Analysis Report, 2026 – 2033
発行元: Grand View Research
URL: https://www.grandviewresearch.com/industry-analysis/machine-condition-monitoring-market-report

１－６．決済端末・自動販売機

課題と解決策

PCI DSS v4.0の厳格な要件に対し、既存端末への**SDKによる後付け保護**（物理RoT）を実装が可能。
物理的なエンドツーエンド保護により、高度なサイバー攻撃やスキミングから決済情報を保護します。

高度なサイバー攻撃
スキミング / 改ざん

PCI要件強化 →

Chip固有識別＋Hashchain
ハードウェアによる保護

完全防御 →

セキュア決済
E2E保護達成

活用事例：決済端末 内部構造

1. **カードリーダー部**
決済情報の読み取り
非接触通信

物理RoT

2. **専用チップ**
データに真正性付与

3. **決済処理部**
データの検証
送信処理

4. **通信部**
ゲートウェイへ
E2E保護された安全伝送

SDKによる後付け保護
カード読み取り直後に専用チップを設置し真正性を付与することで既存システムの大幅な改修なしに強固なハードウェアRoTを実現します。

市場規模データ 決済端末

世界市場	日本市場	米国市場
931.6億ドル	6,840億円	191億ドル

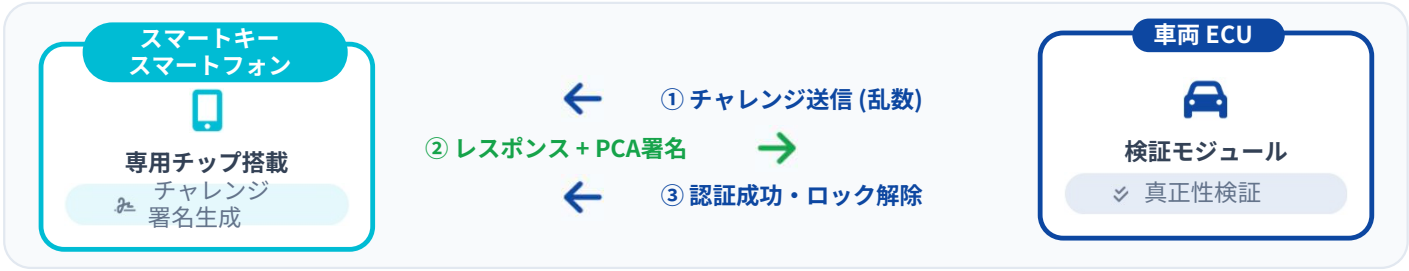
ソース
URL: https://www.mordorintelligence.com/industry-reports/united-states-pos-terminals-market、https://www.datamintelligence.com/research-report/pos-terminals-market、https://www.mordorintelligence.com/industry-reports/japan-pos-terminals-market

１－７．スマートキー・認証キー・無線チップ

課題と解決策

自動車や基幹インフラへのアクセスにおいて、電波を中継する**リレーアタック**による不正解錠・窃盗が深刻な脅威となっています。
スマートキーに専用チップを搭載し、チャレンジ＆レスポンスによる物理認証を行うことで、遠隔地からのなりすましをハードウェアレベルで完全に遮断します。

活用事例：決済端末 内部構造



リレーアタック無効化
中継器（リレー）は車両からのチャレンジ（乱数）に対する正しいSeed情報を生成できないため、認証が失敗し解錠を物理的にブロックします。

市場規模データ

世界市場(2026)	日本市場	米国市場
139.8億ドル	**1,280億円**	**52.3億ドル**

ソース
タイトル: Automotive Smart Key Market Report 2026
発行元: Research and Markets
URL: https://www.researchandmarkets.com/reports/5767490/automotive-smart-key-market-report

2．AI市場

自律社会における「説明責任」の標準

「スマートモビリティ」と「スマートグリッド」を保護する、嘘のつけない伝送経路

1. 絶対的課題：AI分析（ポイズニング防止）とランサムウェア対策としての物理証跡

AIの判断ミス時、**「ロジック不全」か「入力データの物理的改ざん」**かを100%切り分ける説明責任。

スマートモビリティ（自動運転車）の映像、スマートグリッド制御データへのサイバー攻撃・ランサムウェアによる書き換えを物理層で遮断。

AIの判断プロセスを物理的に追跡可能な伝送経路として構築し、改ざんを不可能にする。

2. 国策との連動：広島AIプロセスおよび「信頼できるAI」の物理基盤

政府**「AI戦略会議」**の安全性確保において、センサーや監視カメラの発生源をチップの固有識別で出所を明確化。

「広島AIプロセス」および欧州AI法（EU AI Act）が求めるAI生成物の真正性と透明性に対する技術的回答。

AIの「説明責任」を物理的に保証するための最終的な証拠として機能。

スマートシティの神経系

2－1．スマートモビリティ（V2X）

課題と解決策

自動運転車に対する**走行データや路側センサーデータの汚染**は、AIによる誤判断を引き起こし重大事故に直結します。
V2X環境において、車両と路側機（RSU）間の通信にPCA・ハッシュチェーンを導入することで、改ざんやリプレイ攻撃を物理層から動的に防御します。

活用事例：V2Xネットワークと PCA署名検証システム

リプレイ攻撃防御
車両の専用チップによる動的な物理署名と、RSUでのリアルタイム検証により、過去の正常な通信データを悪用するリプレイ攻撃を完全に排除します。

市場規模データ　Automotive V2X Market

世界市場(2026)	日本市場	米国市場
54.8億ドル	**680億円**	**21.4億ドル**

ソース
タイトル: Automotive Vehicle-to-Everything (V2X) Market Size, Forecast [2023-2035]
発行元: Research Nester
URL: https://www.researchnester.com/reports/automotive-vehicle-to-everything-market/4458

2－2．監視カメラ・防犯監視

課題と解決策

AIによる高度な**ディープフェイクや映像差し替え攻撃**が監視網の無力化を狙っています。
欧州AI法（2024年8月施行）に対応する「物理封印」技術により、カメラ内で1フレームごとに物理検証・署名を行い、真正な映像のみをAI分析サーバーへ伝送します。

活用事例： 映像データのフレーム単位物理封印アーキテクチャ

フレームハッシュ連携

カメラで内の専用チップにおける固有識別情報と各フレームのハッシュ値が連鎖し、途中経路での映像の差し替えや改ざんをAIサーバー側で確実に見破ります。

市場規模データ　ビデオ監視

世界市場(2026)	日本市場	米国市場
950.1億ドル	8,340億円	358億ドル

ソース

タイトル: Video Surveillance Market Size, Share & Industry Analysis Report [2034]
発行元: Fortune Business Insights
URL: https://www.fortunebusinessinsights.com/video-surveillance-market-102673

2－3．ウェアラブル端末・生体認証

課題と解決策

生体認証やマイナンバー連携において、**生体データの改ざんやなりすましリスク**が課題です。
ウェアラブル端末やセンサー自体に専用チップを組み込むことで、データの「発生源」を物理層から証明し、完全な信頼性を担保します。

活用事例： ウェアラブル生体認証経路と物理署名プロセス

エンドツーエンドの信頼

データ発生源であるウェアラブル端末内で物理署名を行うことで、中継経路での改ざんやなりすましを完全に無効化します。

市場規模データ　生体認証市場

世界市場(2026)	日本市場	米国市場
678.6億ドル	5,050億円	206億ドル

ソース

タイトル: Biometrics Market Size, Share Analysis & Growth Trends 2031
発行元: Mordor Intelligence
URL: https://www.mordorintelligence.com/industry-reports/biometrics-market

2－4．ドローン・重機・製造装置

課題と解決策

自律ロボットやドローンの事故時における**責任の所在不明**が課題です。
EU AI責任指令（2024年施行）に対応するため専用チップを搭載し真正なコマンドのみを選別・優先処理し、物理ログによりメーカーの安全配慮義務の履行を証明します。

不正コマンド混入
事故・誤動作の脅威

制御要求 →

Chip固有識別＋Hashchain
真正性・発行元確認

安全稼働 →

監査証跡
EU AI責任指令(2024)対応

活用事例： 自律ロボットの制御データ保護・物理ログ構成

ドローン・重機本体
センサー・アクチュエータ

制御連携 ⇄

制御FCU
専用チップ搭載

1. **コマンド受信**
外部からの指示
→
2. **真正性認証**
送信元の物理情報確認
→
3. **真正命令処理**
不正コマンド排除
→
4. **飛行ログ記録**
ハッシュ連鎖保存

説明責任の証明
不可逆な物理ログにより、事故発生時でも「真正なコマンドに従って動作していたこと」を法的に立証可能。

市場規模データ Autonomous Drone Market

世界市場(2026)	日本市場	米国市場
534.5億ドル	**4,820億円**	**192.5億ドル**

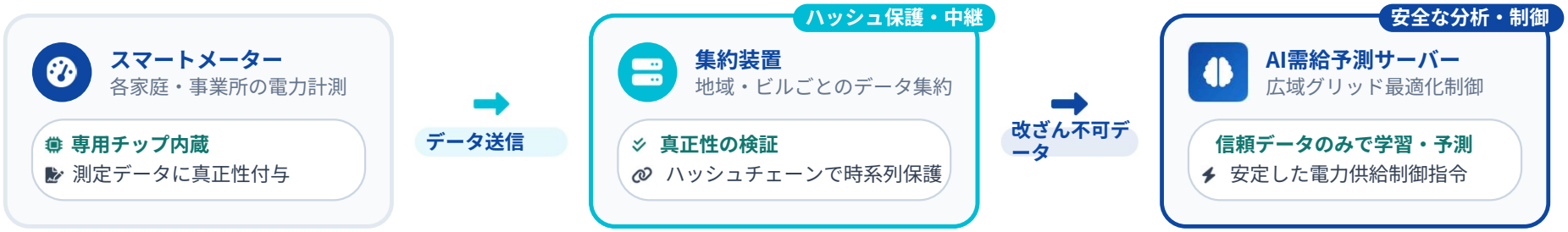
ソース
タイトル: Drones Market Report 2026
発行元: The Business Research Company (Research and Markets)
URL: https://www.researchandmarkets.com/reports/6035243/drones-market-report

2－5．スマートグリッドAI

課題と解決策

AI需給予測システムに対する**悪意あるデータ混入（AIポイズニング）**は、大規模停電を引き起こす致命的なリスクです。
各計測地点からのデータにPCA（チップの固有識別）とハッシュチェーンを付与し、「信頼の連鎖」を構築することでポイズニング攻撃を物理層から完全に遮断します。

活用事例： スマートグリッド「信頼の連鎖」システム



市場規模データ

世界市場(2026)	日本市場	米国市場
525.8億ドル	4,560億円	198億ドル

ソース

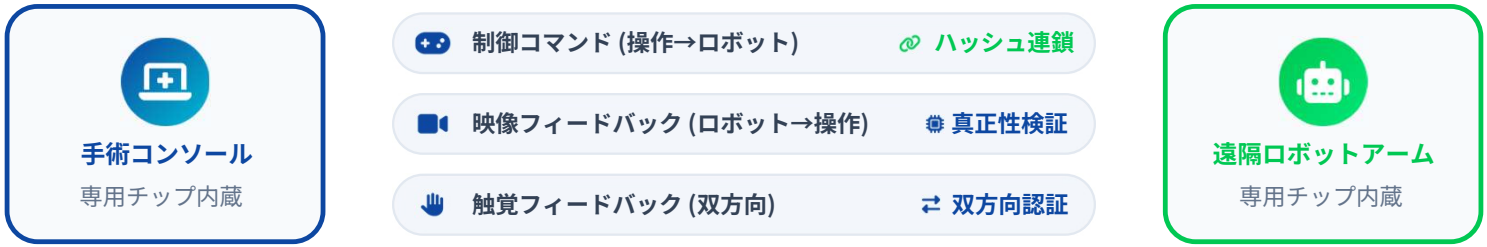
タイトル: Smart Grid Market Size to Hit Around US$ 238.63 Billion by 2035
発行元: Precedence Research
URL: https://www.precedenceresearch.com/smart-grid-market

2－6．AI診断・遠隔手術

課題と解決策

医療DX令和ビジョン2030において、5G/6G環境下でのバイタルデータの**完全性担保**が必須要件です。
医師と患者の真正性を物理チップで鑑定し、誤作動を防止します。遠隔手術ロボットと操作コンソール間の双方向通信をハッシュチェーンで保護します。

活用事例： 遠隔手術システム双方向通信



市場規模データ　5G遠隔手術

世界市場(2026)	日本市場	米国市場
23.5億ドル	340億円	11.2億ドル

ソース

タイトル: 5G Remote Surgery Global Market Report 2026
発行元: The Business Research Company (Research and Markets)
URL: https://www.researchandmarkets.com/reports/6178401/5g-remote-surgery-market-report

2－7．建設機械・ICT施工

課題と解決策

ICT施工において、重機の動線データや施工記録の**改ざんリスク**が客観的な監査の障壁となります。
BIM/CIMデータと紐づく物理施工ログをスクランブルメモリで保護し、国交省ICT施工基準に準拠した改ざん不可能な監査証跡を確立します。

※ BIM/CIM（Building/ Construction Information Modeling）

自己申告データ
改ざんの余地あり

物理的証明 →

スクランブルメモリ
施工ログの暗号化・保護

客観的監査 →

国交省基準準拠
信頼性の高い証跡

活用事例：セキュアICT施工データ連携フロー

建設機械
稼働・動線データ

保護・暗号化 →

ハードウェア保護
スクランブルメモリ
物理検証・署名付与

安全な連携 →

クラウド BIM/CIM
データ統合・検証

自動化 →

監査・支払
信頼性の高い自動処理

BIM/CIM連携の価値
物理的に保護された施工ログにより、3Dモデルデータ（BIM/CIM）の実績値としての信頼性が劇的に向上します。

市場規模データ　スマートコンストラクション/ICT施工

世界市場(2026)	日本市場	米国市場
158.1億ドル	1,450億円	51.8億ドル

ソース
タイトル: Smart Construction Market Forecast 2026–2035 | Growth Trends & CAGR
発行元: Business Research Insights
URL: https://www.businessresearchinsights.com/market-reports/smart-construction-market-120012

３．データ付加価値化市場

2028年「カーボンゼロ」の実現基盤

「スマートグリッド」資産と「インフラ監視」を支えるデータの価値証明

1. 絶対的課題：2028年「炭素賦課金」と金融・健康インフラの「監査証跡」

2028年度開始の**「化石燃料賦課金」**およびEU「CBAM（炭素国境調整措置）」への対応。

自己申告ではない**「検証可能な物理証拠」**によるグリーンウォッシュの排除。

P2P電力取引、地域通貨、ステーブルコイン、マイナンバー連携における物理的な真正性証明。

※グリーンウォッシュ：企業が実態を伴わないのに、環境に配慮しているように見せかけて消費者を誤解させるマーケティング手法

2. 国策との連動：GX経済移行債およびデジタル庁「マイナンバー」構想との親和性

経産省**GX推進戦略**における、測定機器・監視センサー等からのデータを物理鑑定するSDCの役割。

データを**「国際的に換金可能な最高品質の資産」**へ昇華し、ESG投資を呼び込むインセンティブ化。

マイナンバー連携による個人データの物理的保護と真正性証明。

※GX経済移行債（脱炭素成長型経済構造移行債）

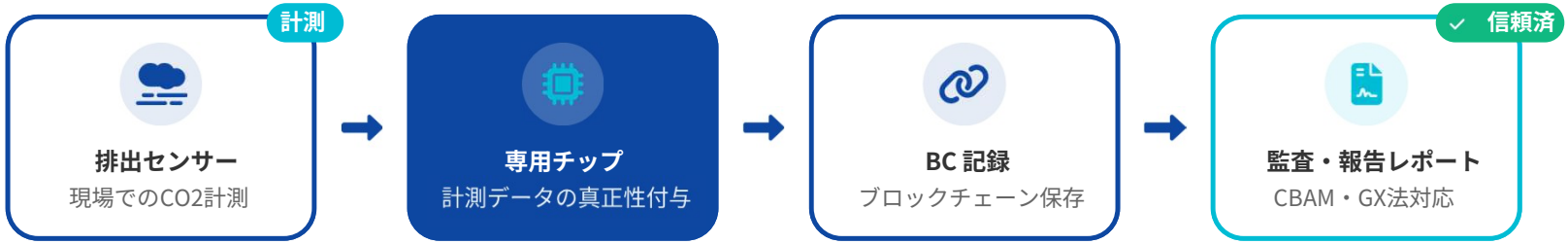
３－１．脱炭素・インフラ監視

課題と解決策

企業が報告する温室効果ガス排出量において、**グリーンウォッシュ（環境配慮の偽装）**が国際的な問題となっています。
排出センサーに専用チップを直結させ、発生源からの物理検証を行うことで、自己申告による改ざんを完全に排除します。

活用事例： カーボンフットプリント（CFP）管理フロー

カーボンフットプリント：商品やサービスの原材料調達から廃棄・リサイクルに至るまでのライフサイクル全体を通して排出される温室効果ガスの排出量をCO2に換算して、商品やサービスに分かりやすく表示する仕組み



市場規模データ

世界市場(2026)	日本市場	欧州市場
168.5億ドル	1,840億円	52.3億ユーロ

ソース

タイトル： Carbon Management Software Market Size, Industry Insights
発行元： Business Research Insights
URL： https://www.businessresearchinsights.com/market-reports/carbon-management-software-market-120668

３－２．スマートグリッド(P2P取引)

課題と解決策

個人間でのP2P電力取引において、自己申告による**再生エネルギーデータの信頼性欠如**が深刻な課題となります。
パワーコンディショナに物理的なチップの固有識別とハッシュチェーンを組み込むことで、売電データにハードウェアレベルの真正性を付与し、セキュアな電力の資産化を実現します。

自己申告データ
信頼性・監査性欠如

計測・送信 →

Chip固有識別＋Hashchain
ハードウェアレベル証明

真正性確保 →

セキュア電力取引
P2Pマッチング成立

活用事例： P2P電力取引システム（V2H・再エネ資産化）

真正性検証　暗号化通信　ブロックチェーン監査証跡

市場規模データ

世界市場(2026)	日本市場	米国市場
109億ドル	**480億円**	**28.5億ドル**

ソース
タイトル： Global Peer-to-Peer Energy Trading Market Report, By Energy Source (Solar, Wind, Others), By Grid Type (Grid-Connected, Off-Grid), By End-User (Residential, Commercial, Industrial), and By Region - Forecast till 2030
発行元： Dataintelo
URL： https://dataintelo.com/report/peer-to-peer-energy-trading-market

3－3．ウェアラブル・ヘルスケア（PHR）

課題と解決策

健康ポイントや治験データの資産化において、**健康データの改ざん不能証明**が求められています。
歩数・心拍データにチップの固有識別とハッシュチェーンで真正性を付与し、PHR利活用ガイドラインに準拠した「物理公証データ」を創出することで、データの経済価値を最大化します。

健康データ改ざん
真正性の欠弱

→ 真正性付与 →

Chip固有識別＋Hashchain
真正性保証

→ 価値化 →

データ資産化
経済価値の創出

活用事例： 健康データ物理公証・連携フロー

ウェアラブル端末
歩数・心拍計測

→ バイタル取得 →

専用チップ
真正性保証

→ ハッシュチェーン →

PHR基盤
ガイドライン準拠

→ 真正性検証 →

保険・ポイント事業者
セキュアなデータ取引

PHRデータ連携

ウェアラブル端末で取得したデータに物理レベルの真正性を付与。改ざん不能な「物理公証データ」として外部事業者へ安全に提供します。

市場規模データ

世界市場(2026)	日本市場	米国市場
120.5億ドル	1,340億円	48.2億ドル

ソース

タイトル： Personal Health Record Software Market Global Report 2026
発行元： The Business Research Company (Research and Markets)
URL： https://www.researchandmarkets.com/reports/5951831/personal-health-record-software-market-report

３－４．在庫/倉庫管理

課題と解決策

物流DXにおいて、データと現物の乖離（棚卸資産不一致）や記録の改ざんが大きな課題です。
物理DX証明を導入することで、RFIDやタグからの入力情報を物理層で署名・検証し、現物一致とトラストチェーンをハードウェアレベルで完全に担保します。

棚卸資産不一致
データ改ざんリスク

解決 →

Chip固有識別＋Hashchain
改ざん不能な通信

現物一致 →

監査・会計連携
透明性の確保

活用事例：物理的RoTに基づく在庫管理フロー

1. **RFID / ICタグ**
   チップの固有識別
2. 読み取り →
   スキャナー/ゲート
   真正性検証
3. データ送信 →
   WMS (倉庫管理)
   改ざんなく記録
4. 連携 →
   監査・会計システム
   完全性の証明

物理的現物一致証明
物品の移動を物理レイヤーで署名し、ブロックチェーン/ハッシュ技術で連続性を担保。確実な棚卸しを実現します。

市場規模データ

世界市場(2026)	日本市場	米国市場
47.7億ドル	**520億円**	**19.1億ドル**

ソース
タイトル： Warehouse Management System (WMS) Market Size & Share Analysis - Growth Trends and Forecast (2026 - 2031)
発行元： Mordor Intelligence
URL： https://www.mordorintelligence.com/industry-reports/warehouse-management-system-market

３－５．マイナンバー連携・VPN

課題と解決策

行政サービスや機密情報へのアクセスにおいて、ID/パスワードの流出による**なりすまし被害**が深刻化しています。
マイナカードのPCAチップとVPNゲートウェイを連携させた物理RoT認証基盤により、なりすましを物理層から完全に排除します。

活用事例：公的認証フロー・VPN連携

市場規模データ

世界市場(2026)	日本市場	米国市場
577億ドル	4,820億円	223億ドル

ソース

タイトル： Digital Identity Solutions Market Size, Share & Industry Analysis
発行元： Fortune Business Insights
URL： https://www.fortunebusinessinsights.com/digital-identity-solutions-market-108829

3－6．IoTファイナンス

課題と解決策

動産担保融資において、機器の実稼働状況や適正な価値の把握（**担保価値不明問題**）が課題です。
重機や製造装置に搭載した専用チップが稼働証跡を物理的に証明します。

活用事例：IoT融資フロー（製造装置・重機）

セキュアファイナンス
物理層から改ざん不可能な稼働データを金融機関に提供。「バーゼルIII」の運用リスク管理要件を満たす高精度な融資を実現。

※バーセルIII：2008年の金融危機を受けて強化された、国際的に活動する銀行の自己資本比率や流動性に関する国際統一基準

市場規模データ

世界市場(2026)	日本市場	米国市場
534.5億ドル	**4,820億円**	**192.5億ドル**

ソース
タイトル: Internet of Things (IoT) in BFSI Market Size, Share & Industry Analysis
発行元: Fortune Business Insights
URL: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-in-bfsi-market-101826

3－7．スマートビル

課題と解決策

ビルの省エネ性能を担保するデータにおいて、改ざんや**グリーンウォッシュ（環境配慮の誇張）**の懸念が指摘されています。
各種センサーの計測データ発生源で物理署名を行うことで、改ざん不可能な監査証跡を構築し、グリーンボンド等の環境認証を強力に支援します。

不透明なデータ
グリーンウォッシュ懸念

計測
収集

Chip固有識別＋Hashchain
発生源での真正性担保

証跡確立

監査証跡
グリーンボンド対応

活用事例：環境債向けBEMS監査システム

- **温度センサー** PCAチップ内蔵
- **照明センサー** 稼働状況記録
- **空調センサー** 消費電力監視

計測・収集
物理署名付与

データ集約・検証

BEMSプラットフォーム
- 署名検証・完全性確認
- 省エネ実績算出

監査連携
改ざん不可データ

監査レポート
グリーンボンド（環境債）対応
信頼性 100% 担保

ビル管理の透明化

物理層で保護されたセンサー群からBEMSへデータを集約。省エネ実績の透明性を証明し、環境投資家からの高い評価を獲得します。

市場規模データ

世界市場(2026)	日本市場	米国市場
525.8億ドル	4,560億円	198億ドル

ソース

タイトル: Smart Building Market Size, Share, Analysis, and Forecast, 2023-2030
発行元: Coherent Market Insights
URL: https://www.coherentmarketinsights.com/market-insight/smart-building-market-5733

Confidential

免責事項（Disclaimer）

■本資料の目的：本資料は一般社団法人伝送データセキュリティ評議会（以下、当評議会）の設立趣意および技術概要、市場予測をご理解いただくために作成されたものです。
■内容の更新：本資料に記載された内容は、発行時点での最新情報に基づき作成しておりますが、今後の国際情勢、技術動向、または標準化プロセスの進捗により、事前の通知なく修正・改訂を行う場合があります。
■将来予測について：記載されている市場予測、売上目標、ロードマップ等の将来に関する記述は、参考文献より引用した予測値であり、その値を当評議会が保証するものではありません。
■著作権および禁止事項：本資料の内容はすべて当評議会に著作権があります。当評議会に無断で、本資料の全部または一部を転載、複製、配布、公衆送信、あるいは二次的に利用することは固く禁じます。また、手段の如何を問わず、本資料をAIの学習、分析、またはコンテンツ生成に供する行為も一切認められません。
■免責：本資料の利用により生じた直接的・間接的な損失や損害について、当評議会は一切の責任を負いかねます。

2026年4月20日 改訂（第五版） 一般社団法人 伝送データセキュリティ評議会