CollaboGate

AIoTを実現するエッジ向け
ゼロトラストセキュリティ

CollaboGate Japan 株式会社
代表取締役 三井正義

CollaboGate

三井 正義

代表取締役

慶應義塾 Keio University　W3C　DIF

2013年	慶應義塾大学 理工学部 物理情報学科卒業
2015年	慶應義塾大学大学院 SFC 修士卒業 デジタル工作機械および自律分散システムに関する研究活動に従事
2015年	ビトム株式会社創業 分散型製造ネットワークを立ち上げ、2017年に撤退
2017年	BC Global Research団体を創設（1,000人規模に拡大） 分散台帳技術の基礎研究開発および多数プロジェクト支援
2019年	CollaboGate Japan 株式会社創業 分散型IDの国際標準化団体 W3C, DIFに加盟
2021年	DIDを活用したIoTセキュリティソリューションを開発 グローバルメーカーのIoTプロダクト開発を支援
2022年	2.3億円シード資金調達を実施 DIF Japan Chairに就任

CollaboGate

Company Summary

会社名	CollaboGate Japan 株式会社
本社	〒105-6415 東京都港区虎ノ門 1-17-1 虎ノ門ヒルズビジネスタワー 15階
代表者	三井正義
設立	2019年5月7日
主な事業内容	エッジ向けゼロトラストデータ基盤 「NodeX」事業
従業員	17人
株主	シードラウンド 2.3億円調達 ITOCHU TECHNOLOGY VENTURES　dnx ventures　LAC

レコード

- 世界初、エッジ向けゼロトラスト基盤を開発
- 国家プロジェクト「Trusted Web」に採択
- 国際標準化団体 DIF Japan Chair 選任

メディア掲載

日本経済新聞　日刊工業新聞　DIAMOND SIGNAL　財界
THE BRIDGE　NEWS PICKS　BUSINESS INSIDER　TechCrunch

パートナー企業

TOSHIBA　PFU A RICOH Company　NR POWER Lab　三菱重工
RICOH　ALSI　FURUKAWA ELECTRIC GROUP　GLORY
RENESAS　intel　Garage+　Google for Startups
aws activate　Microsoft for Startups　W3C　DIF

本講演のポイント

講演概要: 現在、AIとIoTの融合（AIoT）は、製造、医療、スマートシティ、自動車など、さまざまな分野での革新を牽引しています。しかし、AIoTの普及には、データセキュリティと信頼性の確保が欠かせません。本講演では、エッジ環境におけるゼロトラストセキュリティを実現するためのアプローチと課題、そしてその解決策について議論します。

1 AIoTの進展に伴うセキュリティ課題

- AIoTとは？
- IoT環境のセキュリティリスク
- 既存セキュリティモデルの限界

2 エッジ向けゼロトラストセキュリティと課題

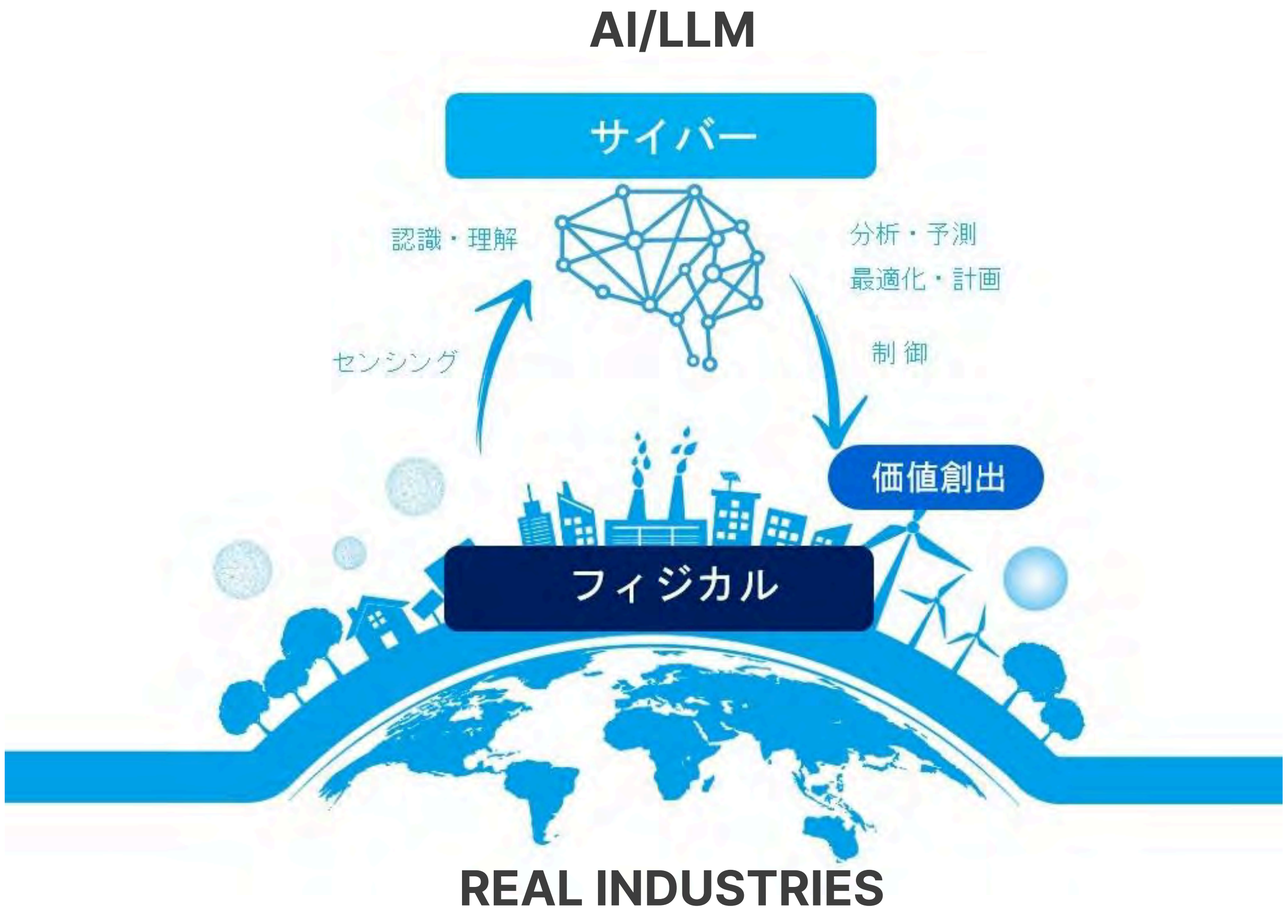
- ゼロトラストの基本概念
- IoT環境での適用に向けた課題

3 分散型IDを用いたアプローチ

- DIDとは？
- IoTセキュリティにDIDを適用するメリット

AIoT

今後、あらゆるモノがインターネットに接続し、データ活用が当たり前になる AI × IoE（Internet of Everything） の時代が到来します。家電、住居、店舗、銀行、道路、病院、空港、農地、工場、国家――日常の暮らしから、国家の防衛に至るまで、あらゆるデバイスがネットワークに接続し、管理され、多くの作業が自動化されていきます。



IoTセキュリティの課題

背景: IoEの普及が進むにつれ、ネットワークに接続されたエッジ端末を標的とするサイバー攻撃が急増しています。特に、セキュリティ対策が十分に施されていないIoTデバイスは、攻撃者にとって格好の標的となり、なりすまし、マルウェア感染、DDoS攻撃の踏み台として利用されるケースが増えています。さらに、攻撃手法の高度化により、個々のデバイスだけでなく、サプライチェーン全体を狙ったサイバー攻撃や、クラウド基盤を標的とした大規模なデータ流出リスクも深刻化しています。

このような背景から、IoTが日常生活から社会インフラ、さらには国家の安全保障にまで広がる中で、セキュリティの重要性はますます高まっています。例えば、スマートホームにおけるセキュリティ侵害は個人のプライバシーに深刻な影響を与えるだけでなく、スマートシティや工場の自動化システムが攻撃を受けると、都市機能の麻痺や生産ラインの停止といった重大な社会的影響を引き起こす可能性があります。さらに、軍事や防衛システムにおいても、IoT技術の活用が進むことで、国家レベルのサイバー攻撃によるリスクが高まりつつあります。

セキュリティ課題: しかしながら、市場には現在、多様なデバイスとデータを包括的に保護できるセキュリティソリューションが不足しているのが現状です。IoTデバイスはメーカーごとに異なる仕様で開発されており、統一的なセキュリティ基準が存在しないため、全体としてのセキュリティ水準がばらついています。このような状況では、企業や組織がデータ活用を進めたくても、セキュリティリスクが障壁となり、IoTの本来の価値を最大限に引き出せていません。IoE時代において、より強固なセキュリティ基盤を構築し、安全にデータを活用できる環境を整えることが急務です。デバイスの認証とデータの完全性を担保するゼロトラストの考え方を取り入れ、エッジからクラウドまでの一貫したセキュリティモデルを構築することが、IoTのさらなる発展と安全な社会実現の鍵となります。

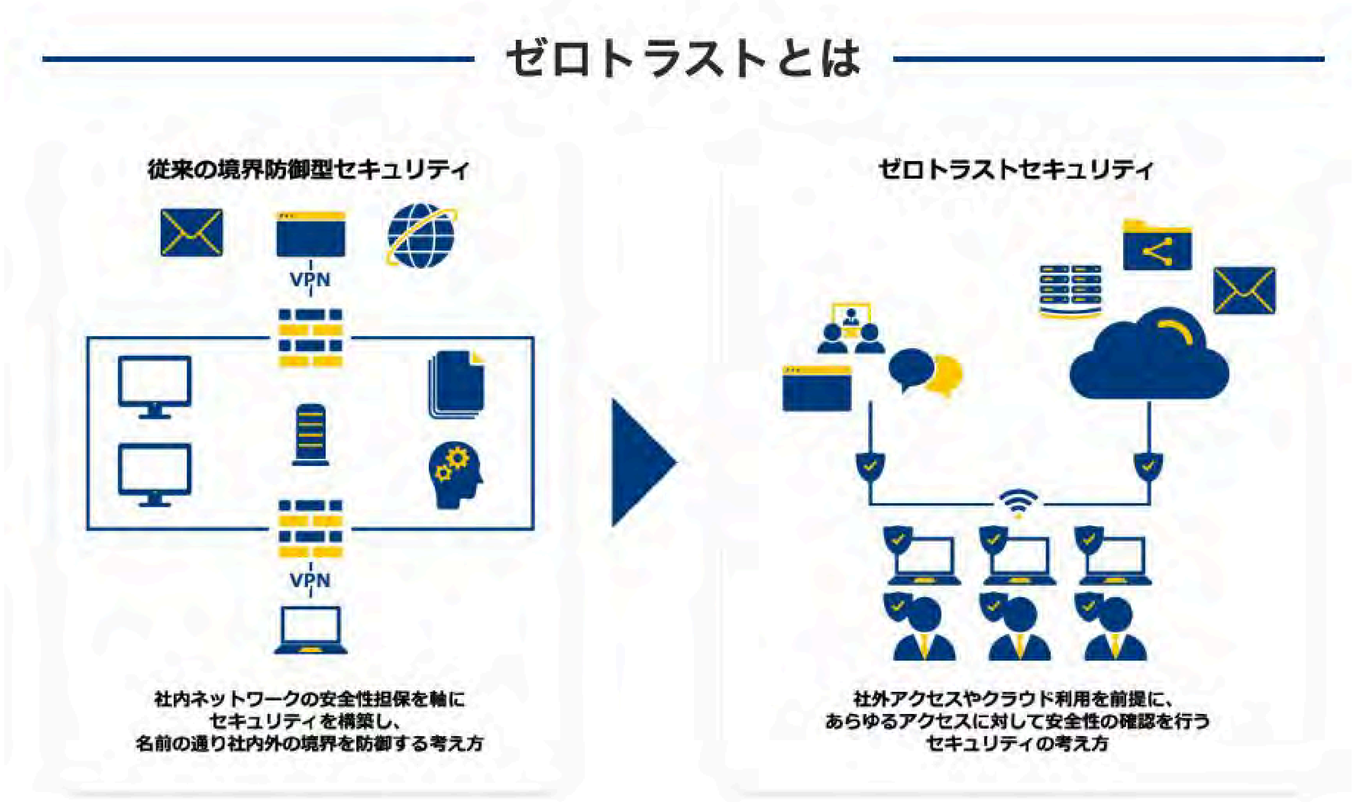
既存セキュリティモデルの限界

オフィスや工場など、機密性の高いデータを扱う施設では、これまで 境界型防御によるセキュリティ対策が主流でした。これは、パブリックネットワークを信頼せず、社内に閉じたネットワークを構築することでデータを守るアプローチです（工場のデータはセンシティブなのでインターネットには繋がないイメージ）。
しかし、この方法にはいくつかの課題があります。

- データが各所にサイロ化し、十分に活用できない（価値のあるデータに必要な人が必要な時にアクセスできない）
- クラウドサービスとの連携が困難 になり、利便性が低下
- 社内不正や内部からの攻撃に対応できない
- マルウェア感染の拡大や、デバイスのなりすましを防ぎきれない
- 専用回線・ファイアウォール・SD-WANなどの追加設備が必要 で、導入・運用コストが増大
- 認証情報やポリシー管理が複雑化し、管理負荷が高まる

これらの課題があるため、従来の境界型防御では、本来の目的であるデータ活用を制限してしまうだけでなく、現代のセキュリティ要件を満たすのが困難になっています。

ゼロトラストのアプローチ



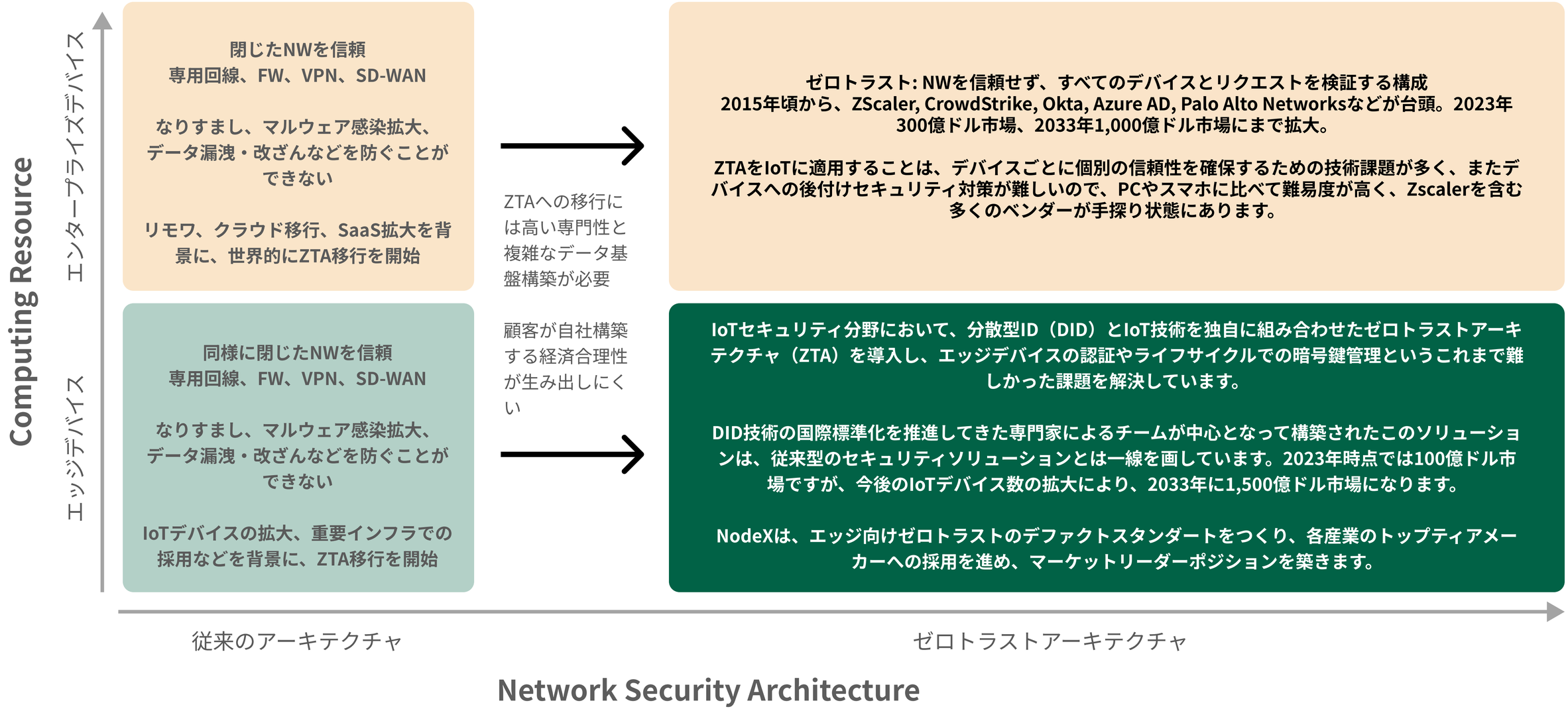
ゼロトラストのアプローチ
これに対し、ゼロトラスト は 「ネットワークを信頼しない」 という前提に立ち、すべてのデバイスとアクセスリクエストを検証することで安全性を確保する アプローチです。
ゼロトラストを導入することで、より柔軟で安全なデータ活用環境を構築できます。

✅ 社内外のデータを安全に活用できる
✅ クラウドサービスとシームレスに連携可能
✅ 従来の境界型防御よりも強固なセキュリティを実現

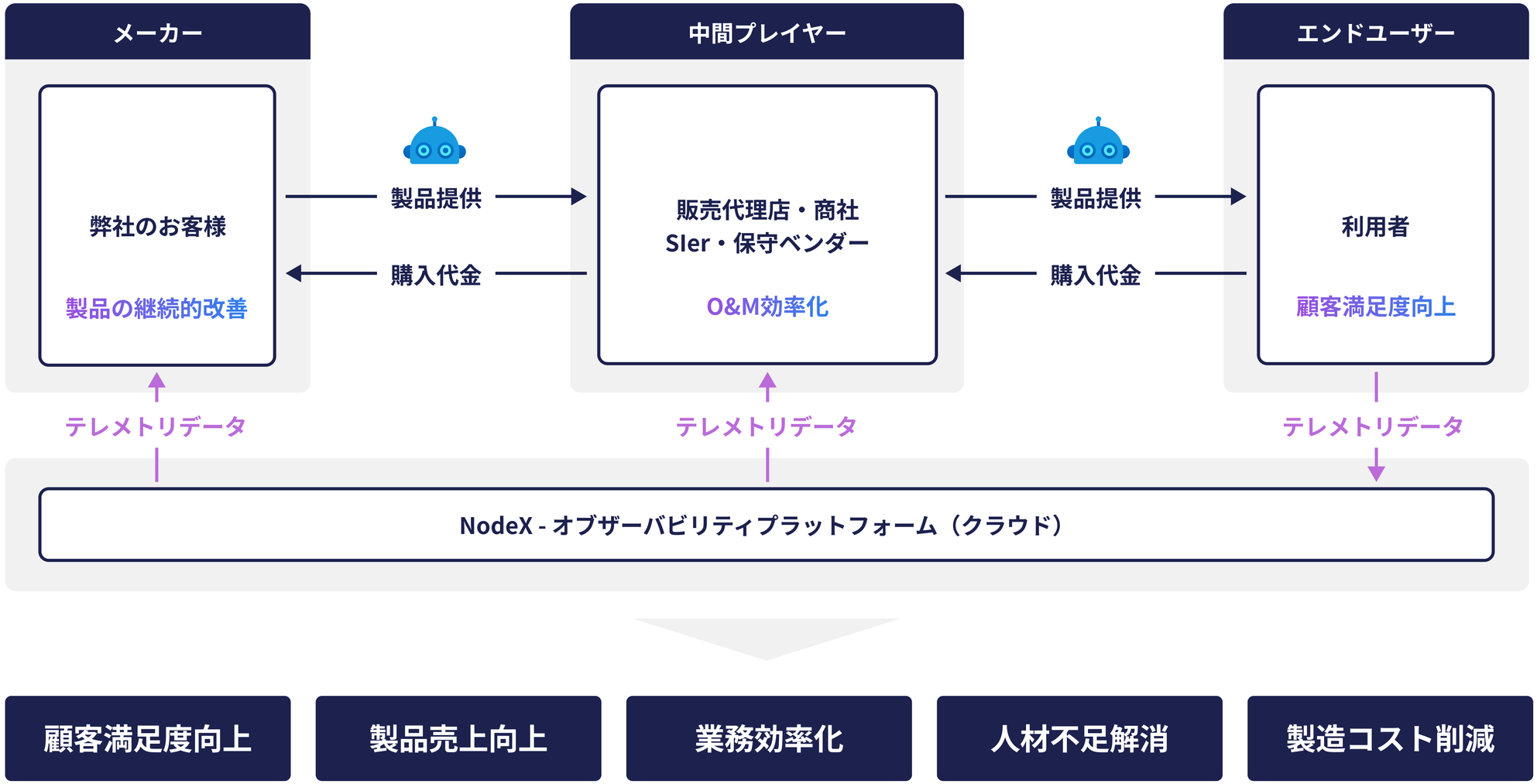
近年、米国政府の大統領令 などをはじめ、世界中の企業や組織がゼロトラストへの移行を進めています。すでにエンプラデバイス（PCやスマホ）領域では、ゼロトラストへの移行を推進するZscalerやCrowdstrikeなど数兆円規模の時価総額になるスタートアップが頻出しています。

NodeXはエッジ向けゼロトラスト製品のリーダー

サイバーセキュリティ界隈の最重要トレンドは「クラウドネイティブ」と「ゼロトラストセキュリティ」です。今後もクラウドに繋がるデバイスが増加し分散する流れは止まらず、世界的なZTAへの移行が必要です。弊社はエッジ向けゼロトラストデータ基盤のマーケットリーダーを目指します。



メーカーはエンドとつながることでさまざまな事業価値を創出



顧客満足度向上　製品売上向上　業務効率化　人材不足解消　製造コスト削減

CollaboGate

しかし、製品データ活用には極めて複雑なインフラ構築が必要

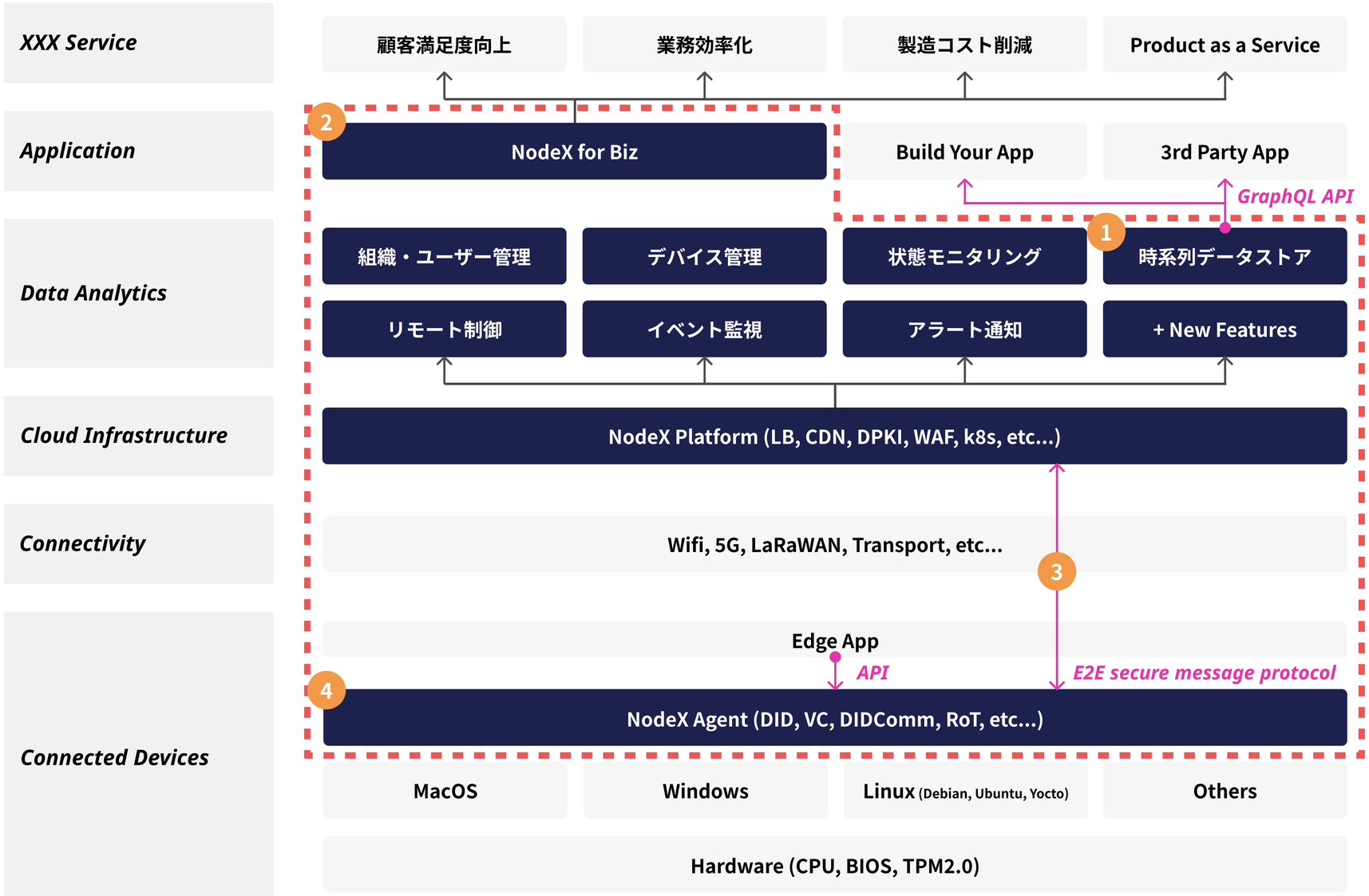
HW選定、エッジアプリ開発、クラウドとのセキュアなコネクティビティ、クラウドインフラ、データ分析基盤、アプリケーション、サービス、、、

XXX Service	顧客満足度向上	業務効率化	製造コスト削減	Product as a Service
Application	アプリケーション			3rd Party App
Data Analytics	デバイス監視	状態モニタリング	リモート制御	データ分析・活用・連携
Cloud Infrastructure	クラウドプラットフォーム (LB, CDN, PKI, WAF, DB, k8s, etc...)			
Connectivity	Wifi, 5G, LaRaWAN, Transport, etc...			
Connected Devices	Edge Application			
	MacOS	Windows	Linux (Debian, Ubuntu, Yocto)	Others
	Hardware (CPU, BIOS, TPM2.0)			

CollaboGate

NodeXは製品データの安全でスケーラブルな収集・分析・活用・連携を支える

製品データを活用したビジネスモデル構築とサービス開発にフォーカスするためのプラットフォームです



1 サービス開発の高速化＆エコシステム構築

製品データを活用したさまざまなサービスをアジャイルに開発できます。御社の既存システムや外部システムとAPI連携することで、エコシステムを構築。

2 オブザーバビリティ

製品テレメトリデータ（メトリクス、イベント、ログデータ）をセキュアに収集し、分析・活用するためのさまざまな機能を開発・提供します。

3 ゼロトラストアーキテクチャ

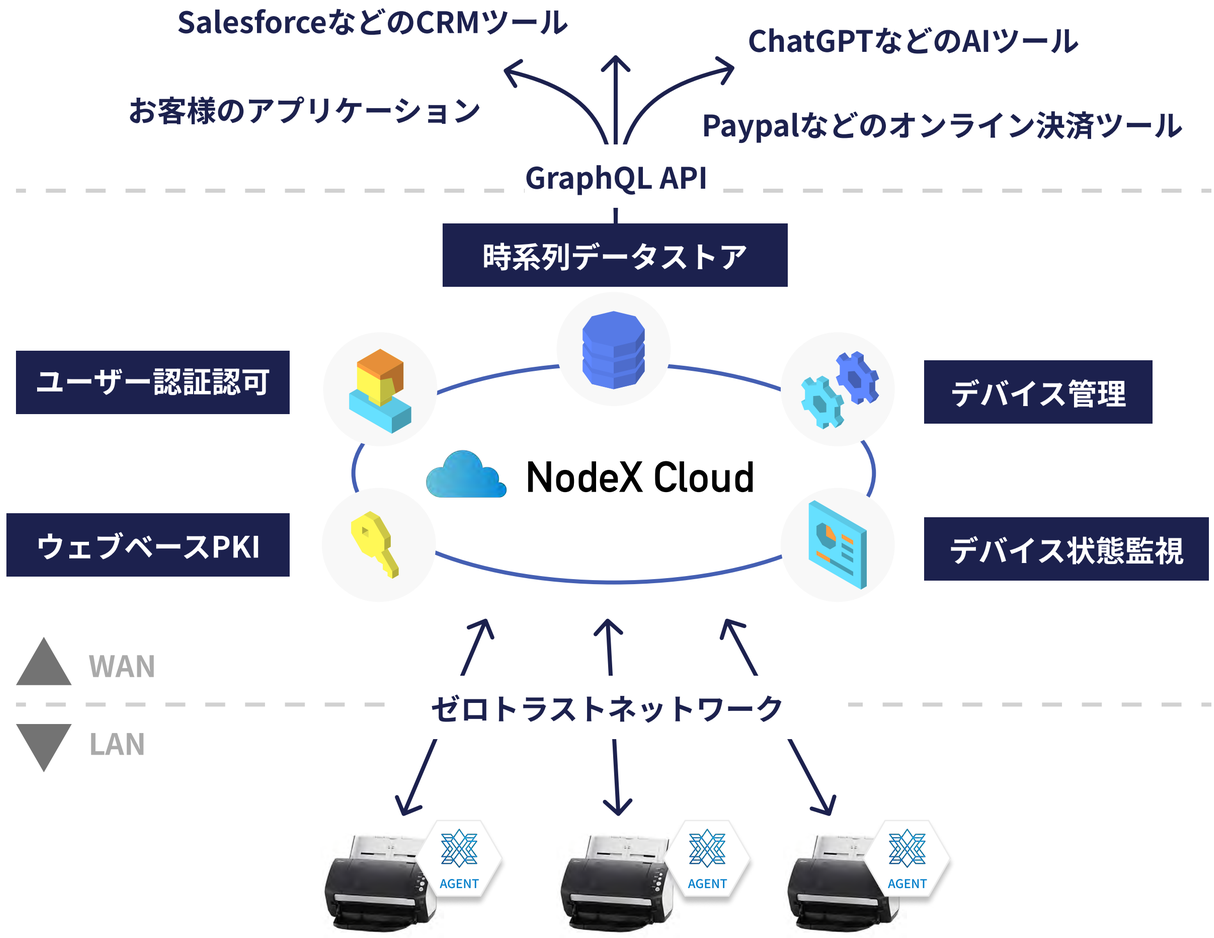
ネットワークを信頼せず、すべてのデバイスとリクエストを検証します。お客様の多様なNW環境に依存せず、安全でスケーラブルなデータ通信を実現します。

4 さまざまなデバイスに統合できるエージェント

W3C標準のDID/VC技術を採用。デバイスの真正性、暗号鍵管理、プロビジョニング自動化、検証可能なメッセージ、トランスポートに依存しないE2EE通信を実現。

NodeX

NodeXのエッジ向けゼロトラストデータ基盤は、さまざまなネットワーク環境で追加のハードウェアやソフトウェアを必要とせず、安全かつ簡単にデバイスデータを収集し、必要な人が必要な時に製品データを利用できるようにします。



NodeX Studio

シンプルで操作性の高いダッシュボード

IoTシステム全体のオブザーバビリティ（可観測性）を確保し、組織横断で共有可能なデバイス管理、テレメトリ監視、アラート機能、運用ダッシュボードを提供します。

NodeX Agent

多様なエッジデバイスに統合できる軽量エージェント（OSS開発）

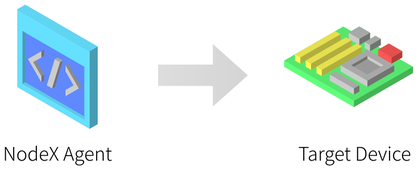
W3C標準の分散型ID技術を採用。デバイスの信頼性、ライフサイクル全体での暗号鍵管理、プロビジョニング自動化、データの検証可能性、トランスポートに依存しないセキュアなE2EE通信を実現。現在、Linux OS, Windows OSに対応。

初期投資を抑え、製品データ活用による事業メリットの創出に伴走

01. NodeX Studioに登録

NodeX Studioにユーザー登録して、プロジェクト（製品）を作成します。

02. 製品にエージェントを統合



エージェントをターゲットデバイスに統合します。現在, Ubuntu, Debian, Yocto, Windows 10 IoT Enterprise で動作するデバイスに統合できます。

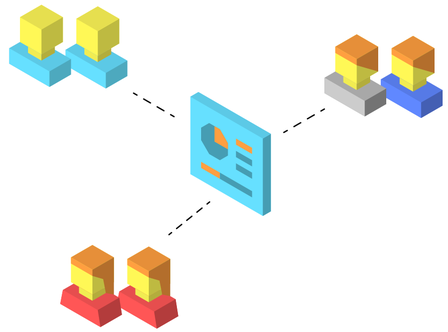
🎥 統合手順動画はこちら

03. テレメトリデータの収集

エージェントからメトリクス、イベント、ログデータをセキュアに収集することができます。お客様の製品に重要なテレメトリデータを収集し、製品開発や保守業務の効率化に役立てることができます。

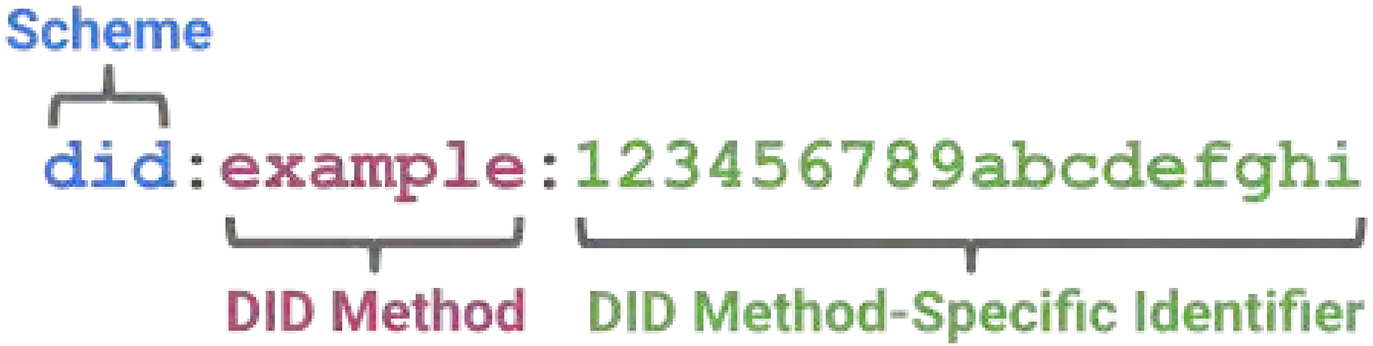
弊社の専門家チームが伴走して、アプリ開発や運用体制の構築までサポートします。

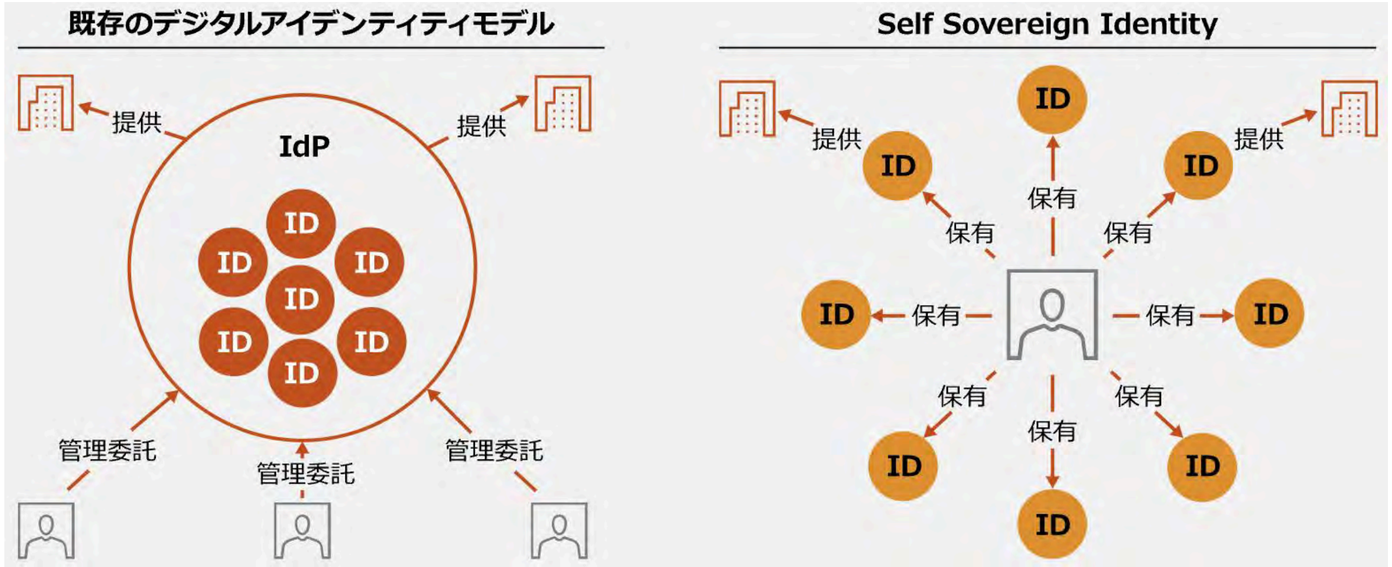
04. 事業メリットの創出



プロジェクトやデバイスグループにユーザー招待することができます。保守事業者とテレメトリデータを共有することで、保守業務の効率化、能動的な保守サービスを提供、顧客満足度を高めます。

DIDとは？

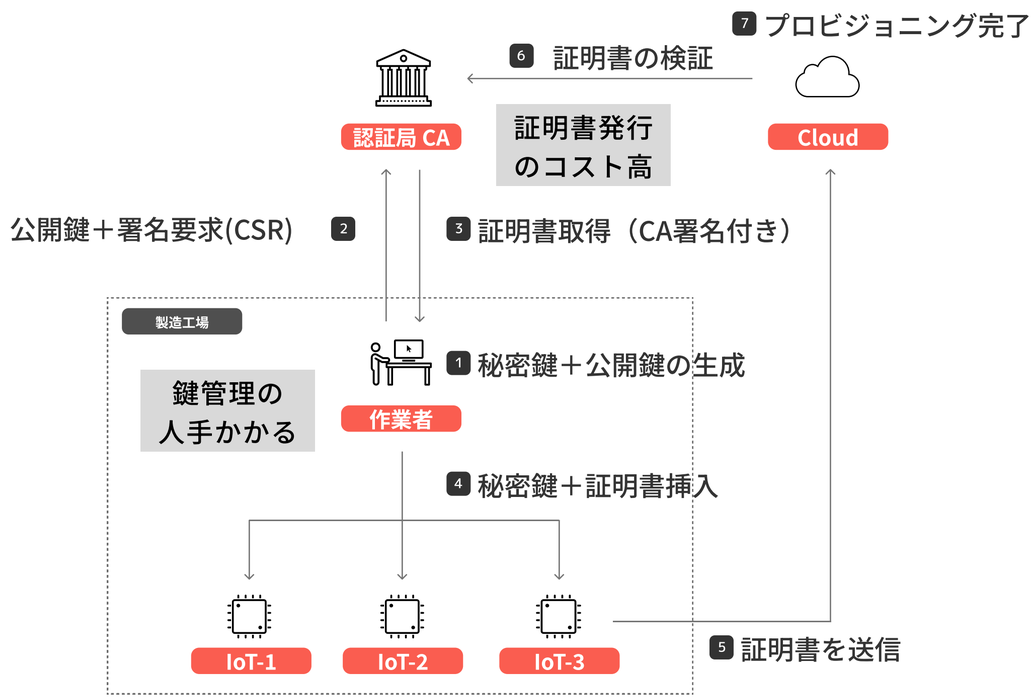




https://www.pwc.com/jp/ja/knowledge/column/disruptive-technology-insights/disruptive-technology-insight13.html

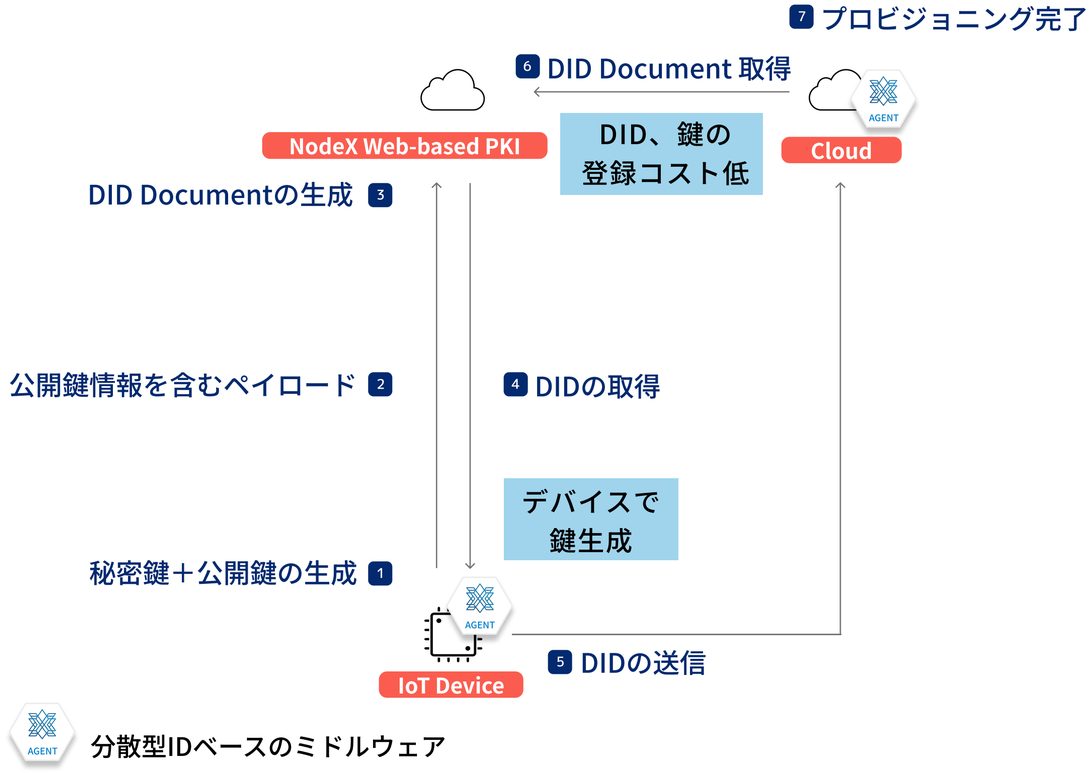
デバイスの信頼性の確保に必要なプロビジョニングの自動化

従来のプロビジョニング



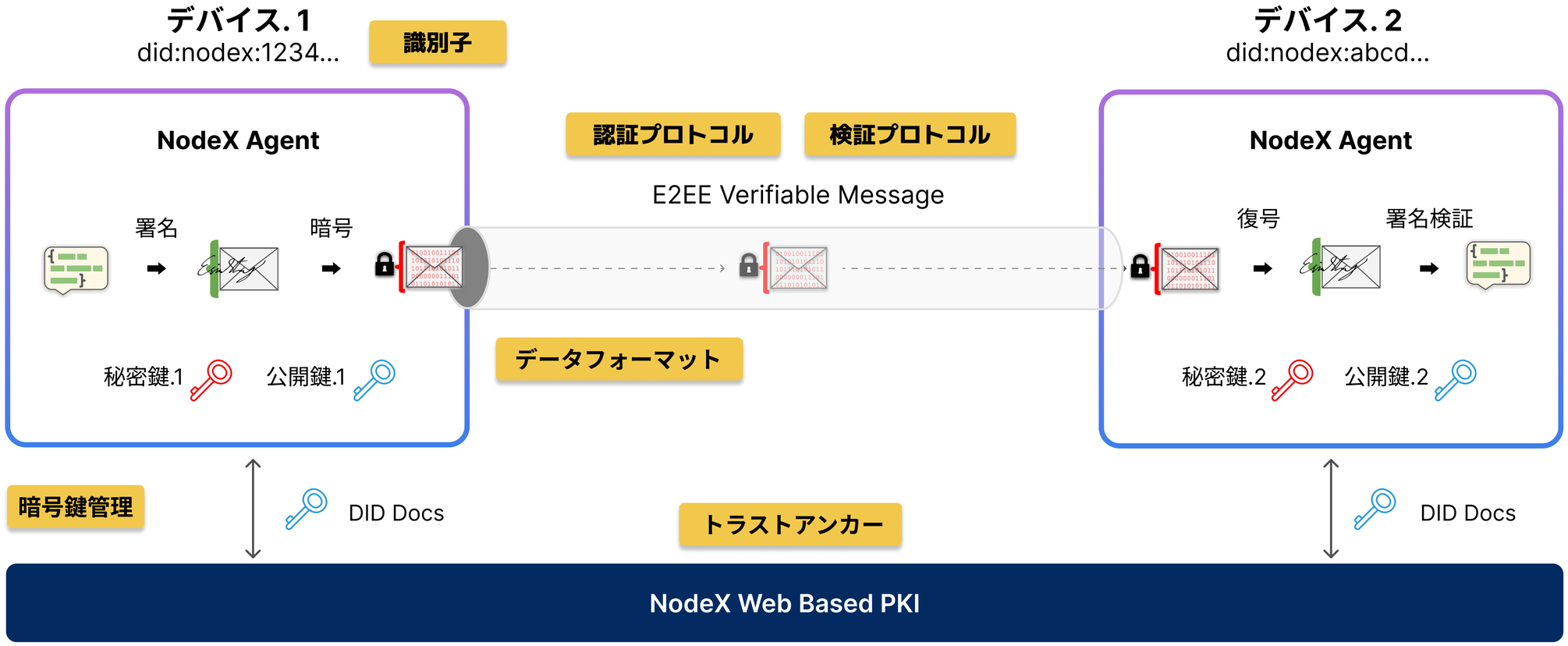
作業者がデバイス外部で暗号鍵ペアを作成し、認証局から証明書を取得、これをデバイスにインストールし管理する手間とコストが発生。プロセスに脆弱性が存在。

自動化プロビジョニング



NodeXエージェントがデバイス内部で暗号鍵を生成し、ウェブベースPKIにDID Document（公開鍵証明書）を登録することでプロビジョニングを自動化。

NodeX - Secure M2M communication protocol based on W3C standard



Our Uniqueness

次世代インフラ技術のパイオニア集団

次世代インフラ技術を世界に先駆けてIoT分野に応用し、グローバルで唯一無二のポジションを構築

World Wide Web Consortium

Web技術の国際標準化を推進する中核的組織.
2022年7月に分散型IDの技術仕様が標準規格に承認.

Decentralized Identity Foundation

分散型IDの国際標準化を推進する中核的組織.
弊社代表の三井がDIF Japan 代表に就任.

Keio Data Architecture Laboratory

インターネットを流通するデータのやりとりのありかたを、データーアーキテクチャ視点で整理し、プロトコルパターンとして整理を行う研究組織. 2023年11月から、弊社「NodeX」のデータ・アーキテクチャおよびOSSと特許戦略に焦点を当てた共同研究を開始.

共同研究の主要メンバー:
村井純（Jun Murai）
慶應義塾大学教授, WIDEプロジェクトFounder, 内閣官房参与（デジタル政策担当）, デジタル庁顧問, KDAL代表・全体統括
鈴木茂哉（Shigeya Suzuki）
政策・メディア研究科特任教授, WIDEプロジェクトボードメンバ, W3C DID WG / VC WG メンバ, KDAL副代表・技術統括