自動車産業におけるデジタルツインのセキュリティ課題と防御手法

TXOne Networks Inc., スレットリサーチ部
シニアスレットリサーチャー, 遠山千鶴

2026年2月10日（火）
制御システムセキュリティカンファレンス2026

Keep the Operation Running

自己紹介 - 遠山 千鶴

- TXOne Networks スレットリサーチ部、シニアスレットリサーチャー
- IT関連脅威のリサーチ、フォレンジックツールの開発 2009-2017 (トレンドマイクロ)
- IoT/OT関連脅威のリサーチ 2018-現在 (トレンドマイクロ、TXOne Networks)
- 現在はOT関連製品の脆弱性リサーチ、脅威インテリジェンスデータの分析をメインに担当。50件以上の脆弱性を発見・報告し、16件のICSアドバイザリーに貢献。

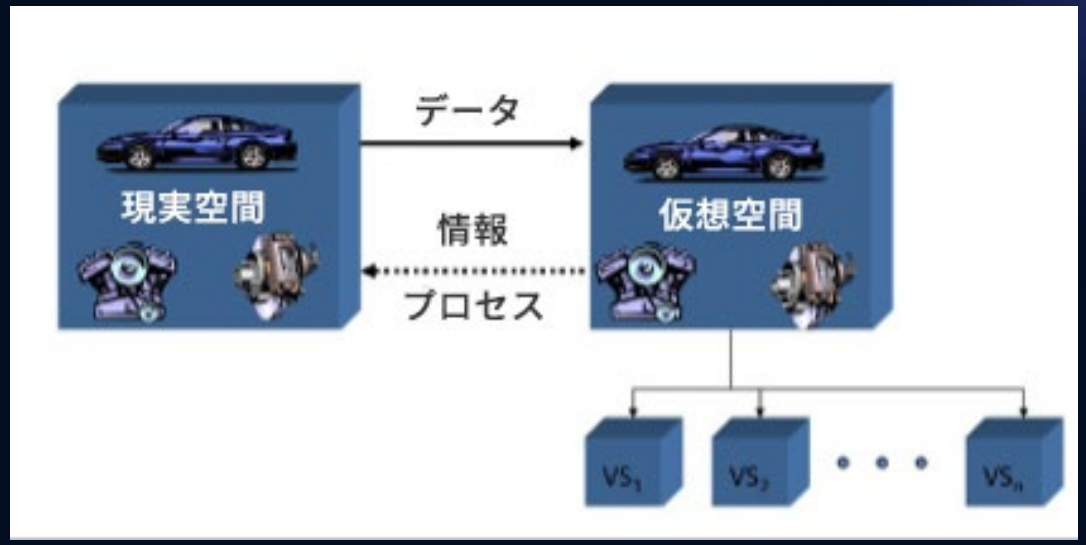
Co-author - Linwei Tsao

- TXOne Networks スレットリサーチ部、スレットリサーチャー
- ICS通信プロトコルおよびネットワークトラフィックの解析を担当。
- 最新のICS攻撃インテリジェンスを収集するため、脅威ハンティングシステムやマルウェア解析ツールの設計・開発・導入を実施。
- ネットワーク関連製品の開発経験あり（モデムファームウェア、DPIエンジンおよびパターン設計）。

目次

デジタルツイン（Digital Twin）の定義と標準

- 定義：現実世界の製品、システム、またはプロセスの仮想モデル。
- 目的：シミュレーション、テスト、監視、保守に利用される。
- 起源：2002年にマイケル・グリーブスがPLMモデルとして提唱。用語は2010年にNASAのジョン・ヴィッカーズによって命名。

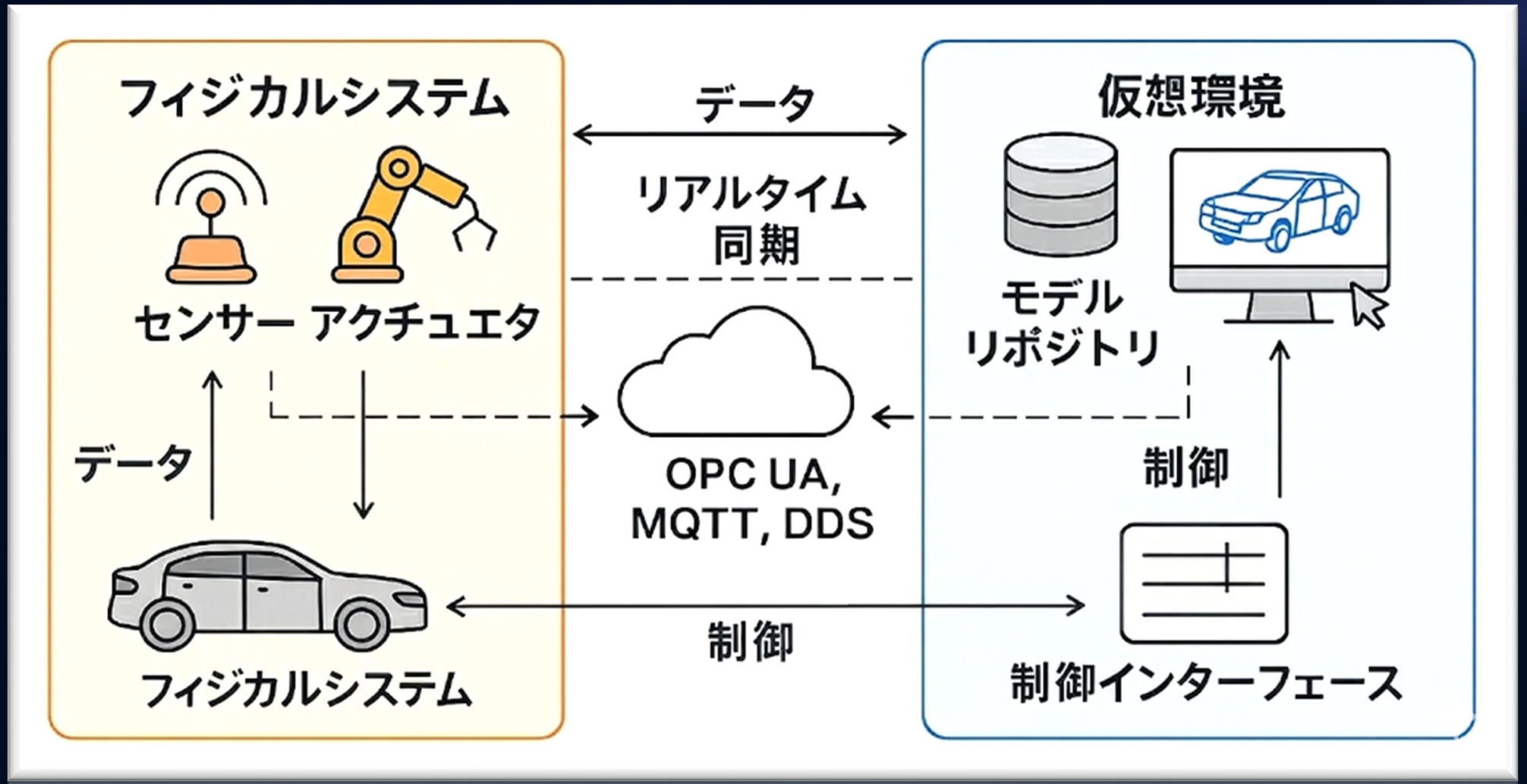


図：デジタルツインの概念とモデル

基本原則（Core Principles）

- 物理システムからのリアルタイムデータを取り込む。
- 制御コマンドを物理システムに送り返す。
- 継続的な同期により、生産と性能を最適化する。

アーキテクチャと運用の全体像



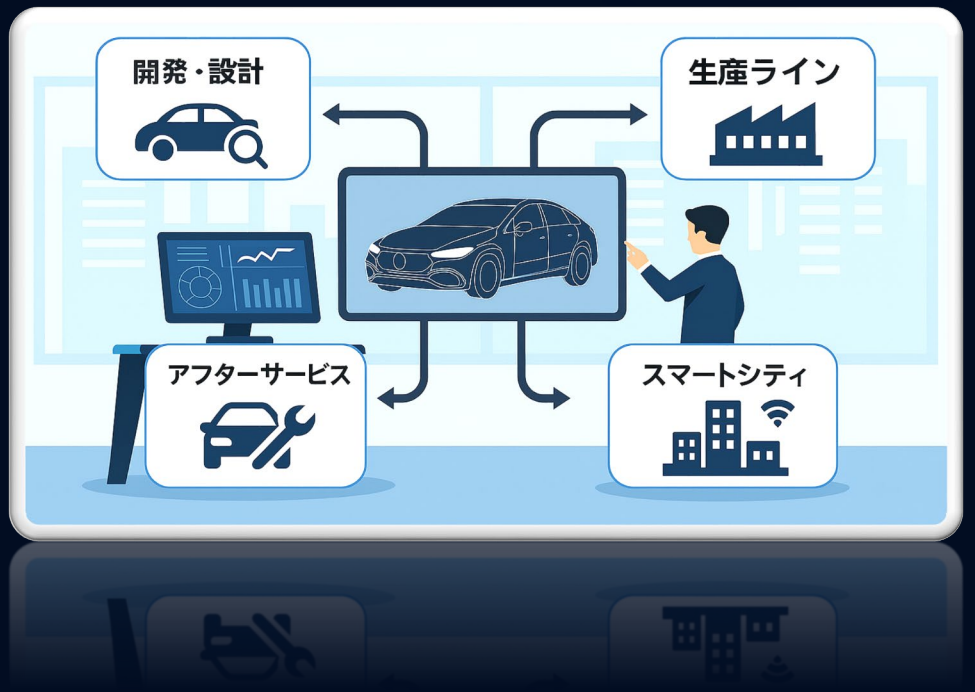
自動車業界でのデジタルツイン活用領域

開発・設計
- 車両・部品の3Dモデルで性能・耐久性をシミュレーション。
- 衝突試験や空力解析を仮想環境で実施。
- EVバッテリーの熱管理・寿命予測。

生産ライン
- 工場設備をデジタル化し稼働率・ボトルネック解析。
- 生産工程の最適化（ロボット・物流）。
- リアルタイム監視で異常検知。

アフターサービス
- 車両状態をクラウドで再現し故障予測。
- OTAアップデート前に安全性検証。
- デジタル車両カルテを提供。

スマートシティ
- 都市交通の渋滞予測・最適ルート計算。
- MaaS運用のシミュレーション。
- EV充電インフラ配置・電力需給予測。



自動車業界の「100年に一度の大変革期」- CASE

Connected（コネクテッド）

- 車両とインターネットを接続し、クラウドや他車との情報共有を可能にする技術。

Autonomous（自動運転）

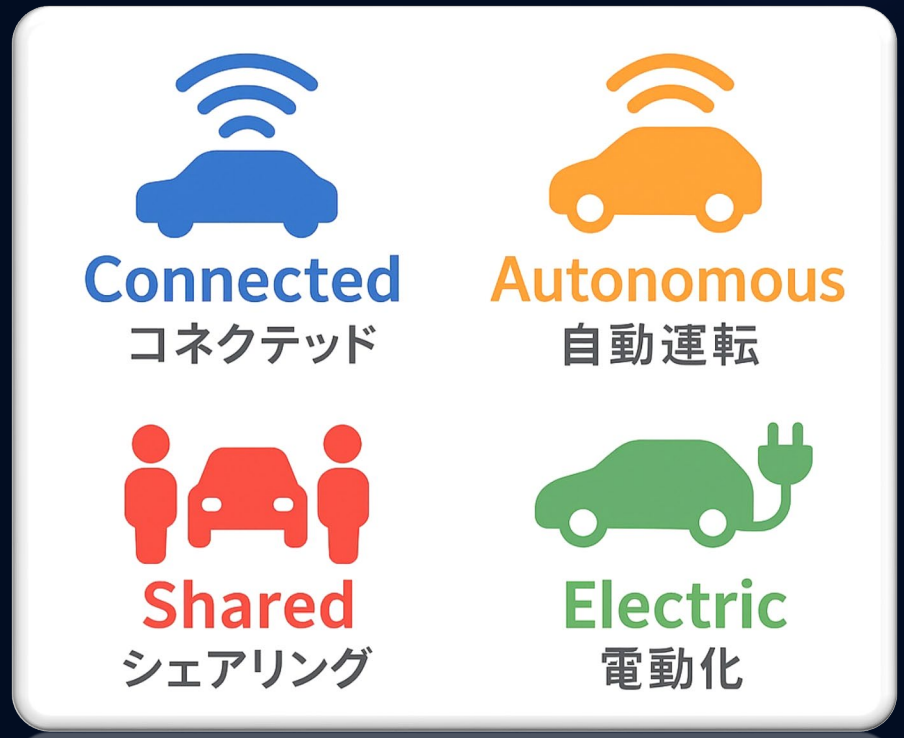
- AIやセンサーを活用し、人間の操作を必要としない自動運転技術。

Shared（シェアリング）

- 車を所有するのではなく、複数人で共有するカーシェアやライドシェアの仕組み。

Electric（電動化）

- ガソリン車から電気自動車（EV）やハイブリッド車への移行による環境負荷低減。



CASEにおけるデジタルツインの役割

CASE	デジタルツインの役割	実現する価値
Connected (コネクテッド)	走行データ・センサーデータ・ユーザーデータをリアルタイム統合・分析、通信遅延のシミュレーション	サービス品質向上、故障予知、OTAアップデートの安全性確保
Autonomous (自動運転)	複雑な交通状況を再現する高精度シミュレーション、自動運転AIの検証	開発コスト・時間削減、安全性最大化、アルゴリズム最適化
Shared (シェアリング)	車両稼働状況やバッテリー残量を仮想管理、効率的な資源計画	シェアサービスの収益性向上、アイドル時間削減、ユーザー待ち時間短縮
Electric (電動化)	バッテリー・エネルギーマネジメント、充電インフラ連携シミュレーション	バッテリー寿命予測、航続距離精度向上、EV生産効率最大化

自動車業界における
デジタルツイン活用事例 🚗

🚗 トヨタ & AIXtal：センサー最適化のためのデジタルツイン

🛠 目的
車両遠隔制御自律走行搬送システム
「Telemotion」におけるセンサー配置の自動化

🏗 仕組み

- ✓3Dデジタルツインでトヨタの量産工場を再現
- ✓物理的な導入前に、安全性・コスト・カバレッジを評価

✅ メリット
試行錯誤を削減、コスト低減、安全性向上

🚀 インパクト
新しいプロセスへの迅速な適応を可能にし、ゼロ事故ビジョンを支援

「デジタルツイン環境で再現したトヨタ自動車の量産工場」

「Telemotionを活用した自律走行の様子」

出典：AIXtal公式ニュース「トヨタにおけるセンサー最適化のためのデジタルツイン」
https://aixtal.com/news/20251008toyota_motor/

🚗 Honda：エネルギー管理におけるデジタルツイン活用

🛠 目的

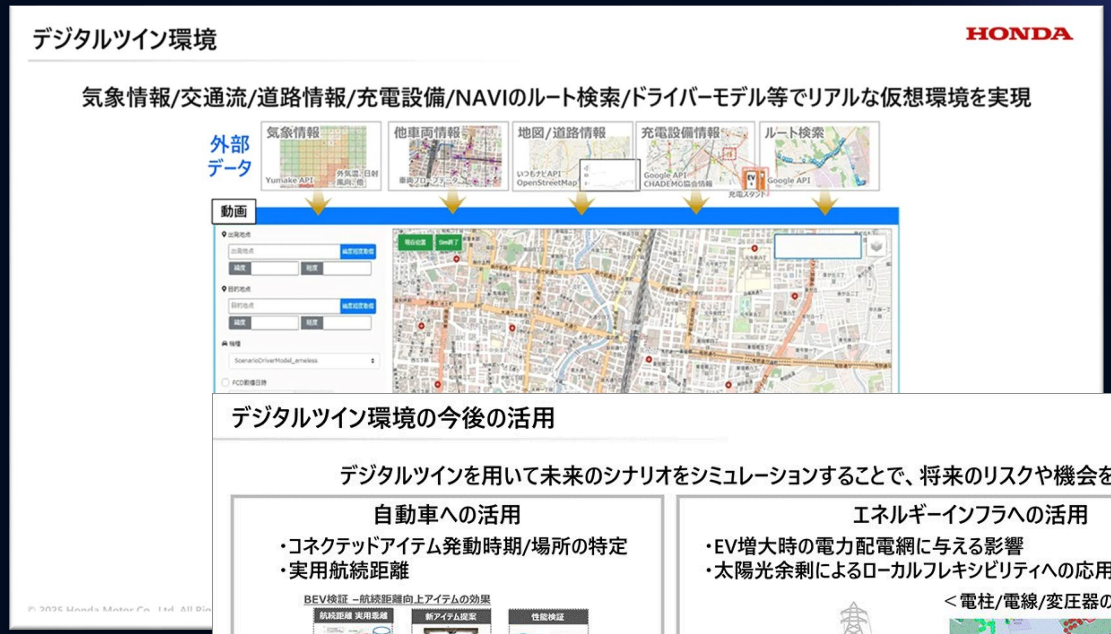
- ✓ EVと再エネを統合し、V2G/V1G戦略を最適化
- ✓ 災害時やピーク時の電力供給を安定化

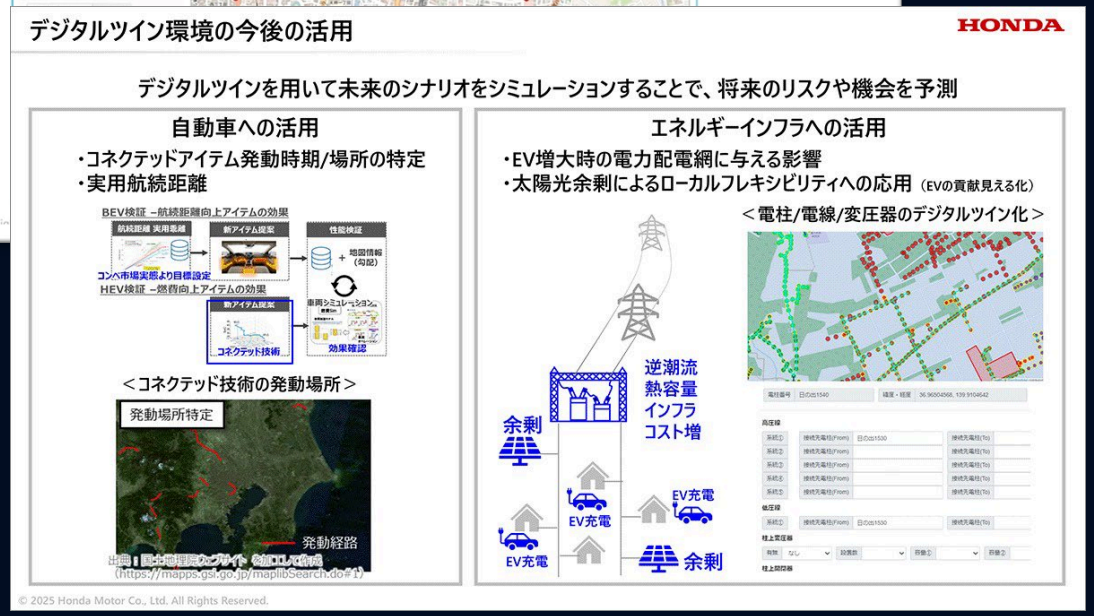
🔍 仕組み

- ✓ 天候・交通・充電設備を統合した仮想モデルで運用検証
- ✓ バッテリーSOC/SOH予測による充放電最適化
- ✓ データ駆動で需給バランスをリアルタイム調整

✅ メリット

- ✓ V2G/V1G戦略を事前検証し、実装リスクを低減
- ✓ バッテリー寿命を延ばし、EV価値を最大化
- ✓ 分散型再エネ社会への移行を加速





出典：Honda公式サイト「生産技術におけるデジタルツイン活用」
https://software.honda-jobs.com/article/43/

🚗 Hyundai：Metaplant America（最先端のスマート工場）

🛠 目的
米国でEV生産を加速し、持続可能なモビリティと地域経済成長を推進。

🏗 仕組み

AI・スマート製造技術とデジタルツインを活用し、ロボット・自動搬送・リアルタイムデータで効率化。

✅ メリット

年間最大50万台の生産能力、品質向上、コスト削減、柔軟な生産対応。

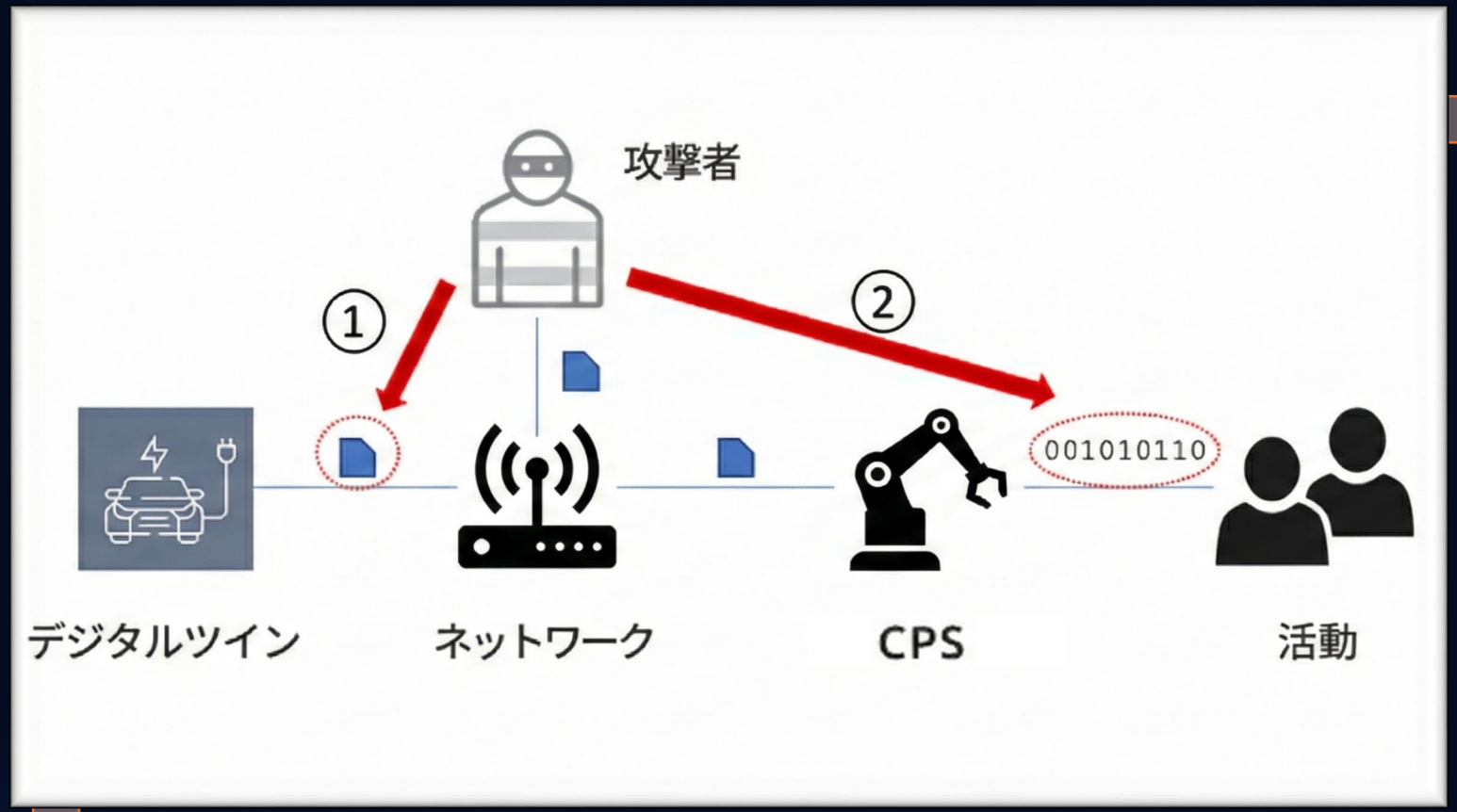
🚀 インパクト

メタプラントおよび関連企業を含め、地域における大規模な雇用を支援。

出典：Hyundai公式ニュース
https://www.hyundai.com/worldwide/en/newsroom/detail/hyundai-motor-group-metaplant-america-celebrates-grand-opening%252C-powering-u.s.-economic-growth-0000000920

想定される攻撃シナリオ 🔓

攻撃シナリオ①：ネットワーク偵察

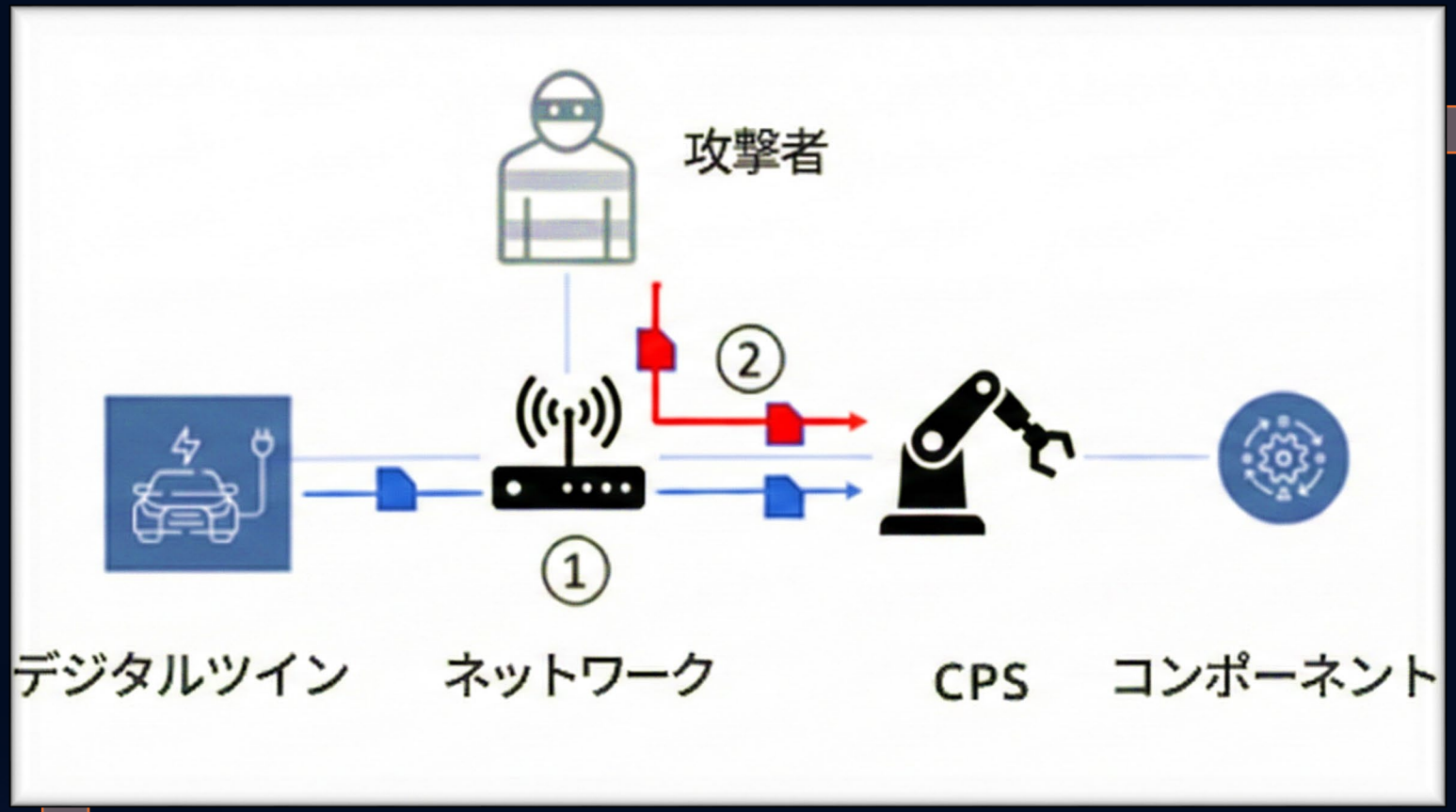


1、デジタルツインとCPS間の通信帯域を検出。

2、CPSの活動を認識。

3、得られた情報からシステムの動作を推測。

攻撃シナリオ②：データインジェクション

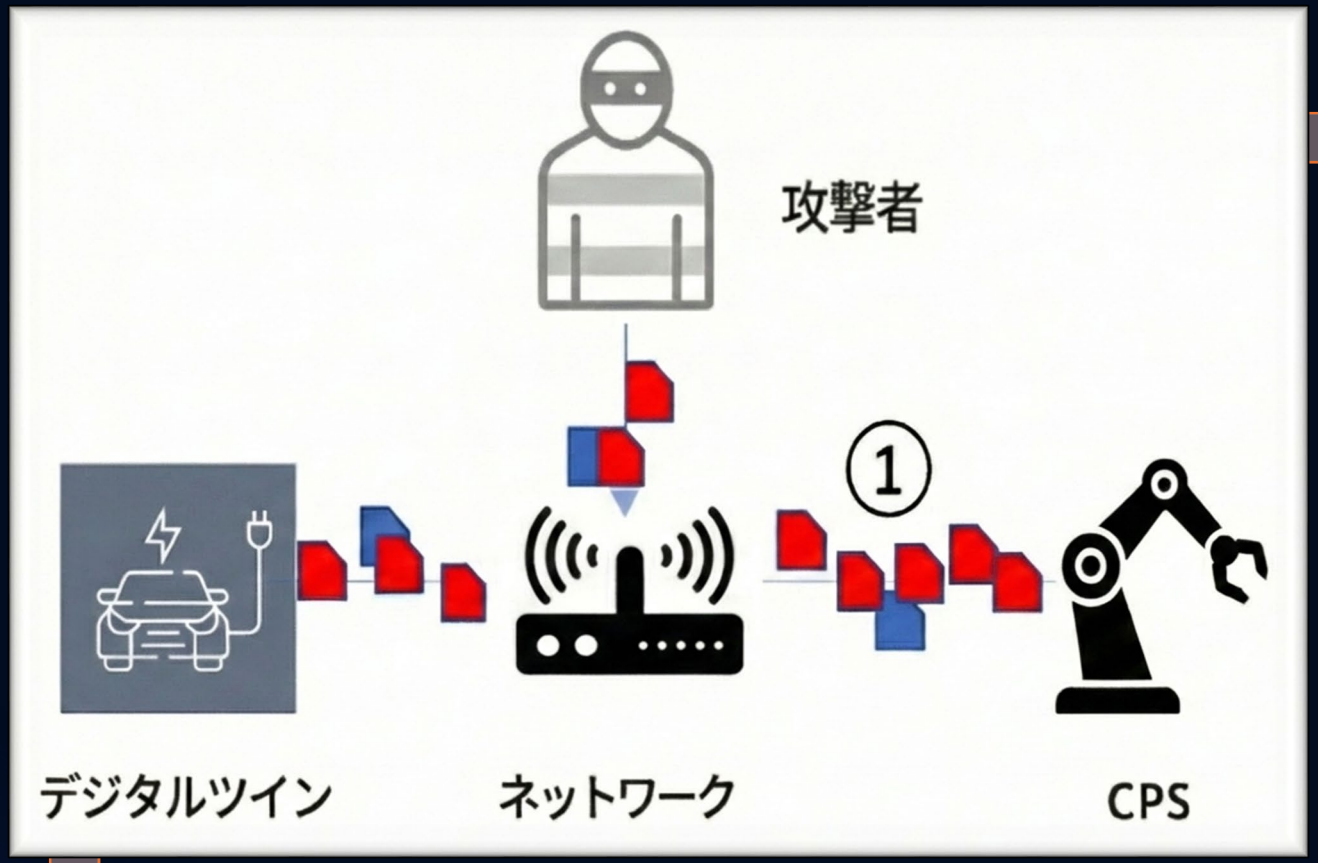


1、デジタルツインからCPSへ正規コマンド送信

2、攻撃者からCPSへ偽コマンド送信

3、CPSが混乱し、同期が崩れる

攻撃シナリオ③：遅延攻撃（リアルタイム阻害）

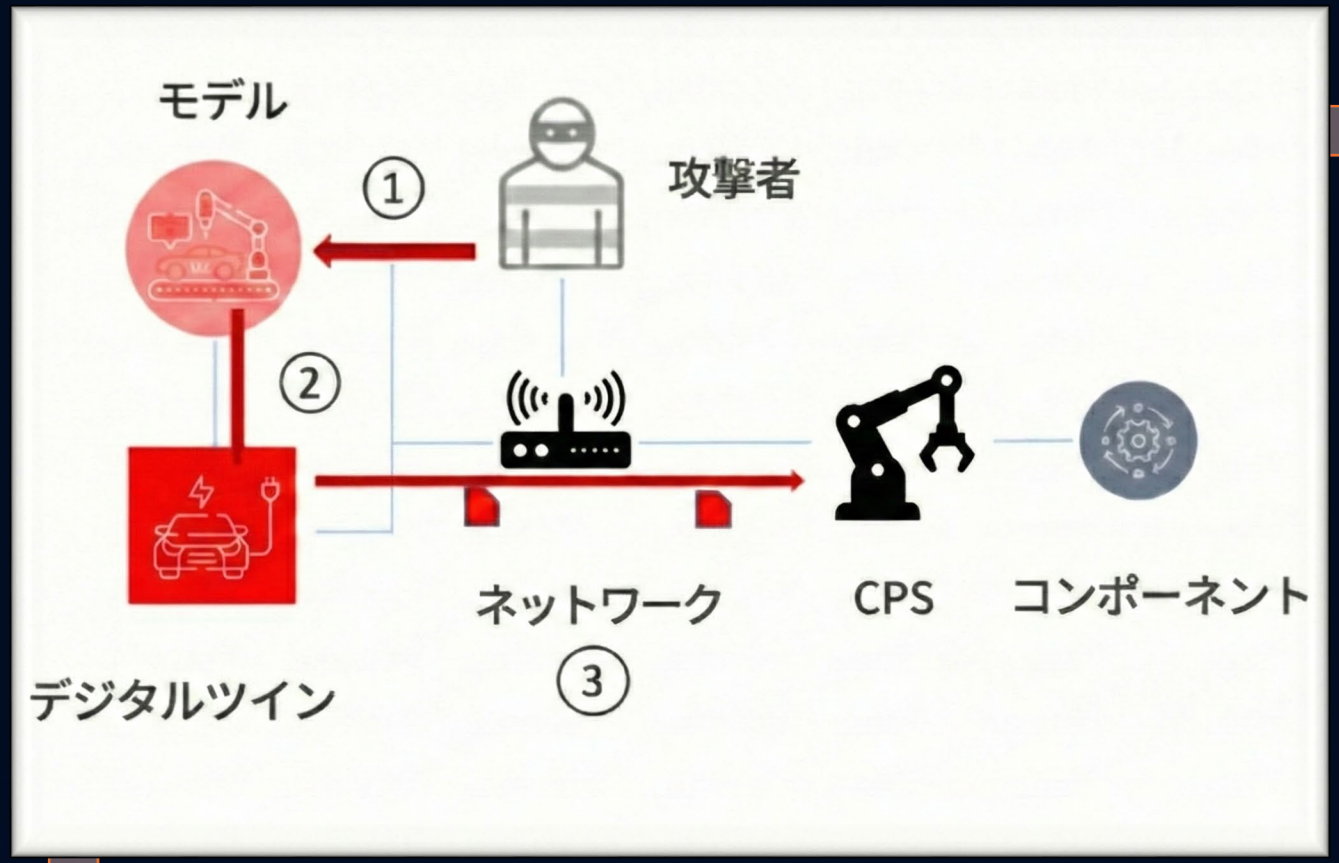


１、攻撃者が大量のランダムトラフィックを発生

２、ネットワークが混雑し、通信が遅延

３、CPSやデジタルツインがデータを受信できず、タイムアウト発生

攻撃シナリオ④-1：モデル改ざん（仮想側への侵入）

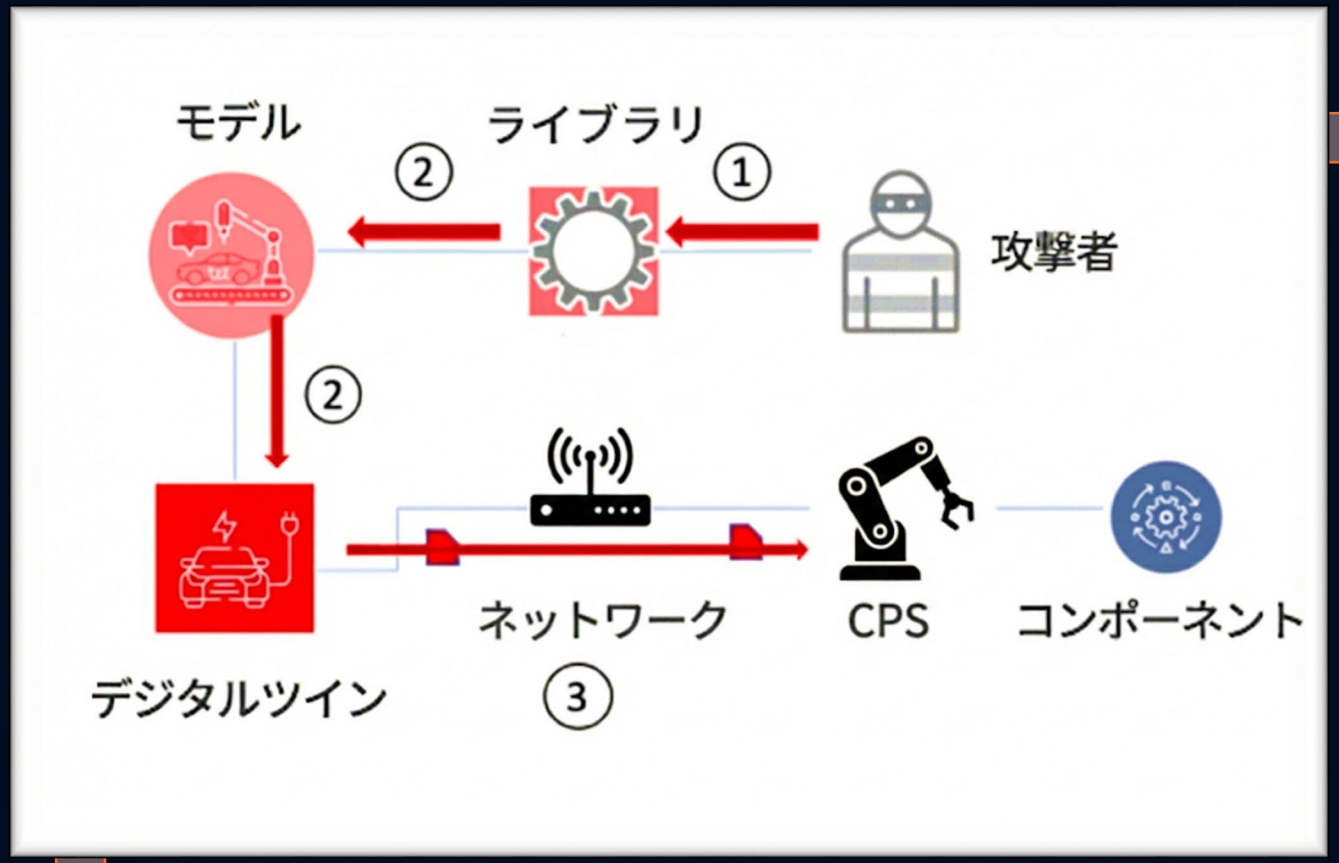


１、モデルへアクセスし、悪意あるコードを注入

２、悪意あるコードがデジタルツインに注入

３、CPSに偽データを送信

攻撃シナリオ④-2：モデル改ざん（ライブラリへの侵入）



1、ライブラリへのコード注入

2、モデルを経由してデジタルツインが感染

3、CPSに偽データ送信

リスク評価とロール別防御策 🛡️

Keep the Operation Running

リスク評価・影響分析

攻撃タイプ	侵入経路	物理システムへの影響	検知難易度	リスクレベル
ネットワーク偵察	ネットワークスキャン／プロトコル解析	攻撃準備段階でシステム情報漏洩、後続攻撃の精度向上	中	低
データインジェクション	センサーインターフェース／ネットワーク	CPSの判断誤り、品質低下	高	高
遅延攻撃	ネットワーク層	タイムアウト、運用停止	中	中
モデル改ざん	クラウド／モデルリポジトリ	制御ロジックの誤動作、ロボットの危険な動き	高	高

対策の技術的評価（有効性／限界）

攻撃フロー	主な対策	有効性	限界
ネットワーク偵察	○ ネットワークセグメンテーション ○ IDS/IPS導入 ○ 異常通信検知 ○ ログ可視化	高：初期偵察の可視化・ブロックが可能で、早期段階で阻止しやすい	✓ ステルス偵察は検知困難 ✓ 誤検知による運用負荷 ✓ 暗号化通信の可視化限界
データインジェクション	○ データ入力検証 ○ AIモデルの入力フィルタリング ○ データ整合性チェック	中：明らかな改ざんや異常値の混入を抑制し品質を維持できる	✓ 巧妙な偽装は通過し得る ✓ リアルタイム検証が難しい
遅延攻撃	○ 制御システム監視 ○ AGV動作異常検知、 ○ フェイルセーフ/冗長化設計	中：異常動作の早期検知と安全停止で被害拡大を抑制	✓ 物理的妨害は検知困難 ✓ 停止に伴う生産影響 ✓ 復旧に時間と調整が必要
モデル改変	○ モデル署名・ハッシュ検証 ○ アクセス制御、変更管理(MOC) ○ モデル更新時の検証プロセス	高：改ざんモデルの検出に有効、変更履歴のトレーサビリティ向上	✓ 内部者攻撃や権限濫用には弱い ✓ 改ざん検知後の復旧コスト大

攻撃シナリオと役割(例)

攻撃フロー	主担当 (R)	協力 (C)	監視 (SOC)	報告先 (A)
ネットワーク偵察	OTセキュリティチーム	OTネットワーク, DTアーキテクト	OT SOC, IT SOC	CISO, OT責任者
データインジェクション	データエンジニアチーム	DTモデラー, AIセキュリティ	OT SOC, AI SOC	CISO, AI責任者
遅延攻撃	OTセキュリティチーム	設備保全	OT SOC	CISO, OT責任者
モデル改変	AIセキュリティチーム / DTアーキテクト	AIエンジニア, DTモデラー	AI SOC, IT SOC	CISO, AI責任者

インシデント対応プレイブック(例)（ロール×シナリオ）

	検知	初動対応	封じ込め	報告	証拠管理	復旧
ネットワーク偵察	OT SOC / IT SOCで異常スキャン検出	OTセキュリティチーム調査、協力：OTネットワーク・DTアーキテクト	不審IPブロック、ネットワークセグメント隔離	CISO、OT責任者	ログ保存、フォレンジック準備	脆弱性の修正、ファイアウォール設定の見直し、IDS/IPSルール更新
データインジェクション	OT SOC / AI SOCで異常データ検出	データエンジニア部門確認、協力：DTモデラー・AIセキュリティ	データストリーム停止、改ざんデータ隔離	CISO、AI責任者	ログ保存、フォレンジック準備	バックアップデータからのリストア、データの整合性チェック
遅延攻撃	OT SOCで工程異常検出	OTセキュリティチーム現場確認、協力：設備保全	異常遅延を発生させている通信源／経路の遮断・分離	CISO、OT責任者	制御ログ保存	生産工程の再スケジュール、制御システムの校正
モデル改変	AI SOCでモデル異常検出	AIセキュリティチーム検証、協力：AIエンジニア・DTモデラー	改ざんモデル隔離	CISO、AI責任者	モデル改変履歴保存	学習済みクリーンモデルへの差し替え、再学習環境のセキュリティ強化

デジタルツイン活用におけるライフサイクル全体のセキュリティ設計①

1. 企画・要件定義

- 重要資産（制御ロジック／製造データ／AIモデル）の識別
- DT固有リスクの洗い出し（整合性低下・データ汚染・遅延攻撃）
- 基準：ISO/SAE 21434、IEC 62443、NIST DT Framework

2. アーキテクチャ設計

- データフロー・境界保護（IT/OT/Cloud 分離）
- モデル整合性メトリクス（精度／遅延／同期率）
- ID／証明書ベースのアセット認証

3. 実装（開発）

- 安全なモデル／シミュレータ開発（SBOM、SAST/DAST）
- データ署名・暗号化、AI学習データの汚染対策
- 誤差注入・モデル汚染攻撃への耐性設計

4. 検証

- DT×物理ラインの整合性テスト
- サイバー・フィジカル統合テスト
- DT環境を使った攻撃シナリオ演習

デジタルツイン活用におけるライフサイクル全体のセキュリティ設計②

5. 展開

- OTゾーン内の適切配置（DMZ、ゼロトラスト）
- モデル／パラメータ更新のセキュアデプロイ
- 鍵・証明書管理の強化

6. 運用

- DT↔実ラインの乖離監視（ドリフト検知）
- OT SOCによる異常検知
- インシデント対応：DTで影響範囲を即時シミュレーション

7. 維持管理

- パッチ管理、モデル更新のバックテスト
- ログ・生産履歴・判断ログの長期保存
- 継続的整合性モニタリング

8. 廃止

- 機密データ・AIモデルの安全な削除
- DT関連アカウント・鍵の完全廃棄
- 生産設備の構成情報・ツイン連携情報の除去

✅まとめ

1. デジタルツインの重要性
   - 自動車産業における開発・生産・運用の効率化と安全性向上に不可欠。
   - CASE（Connected, Autonomous, Shared, Electric）領域での活用が加速。
2. セキュリティ課題
   - 双方向同期による攻撃面の拡大。
   - 主な脅威：ネットワーク偵察、データインジェクション、遅延攻撃、モデル改ざん、情報漏えい。
3. リスク評価
   - 誤制御や生産停止、品質低下、知的財産流出は非常に高リスク。
   - データインジェクションやモデル改ざんは検知困難で長期影響。
4. 防御戦略
   - 領域特化型の多層防御と限界の把握。
   - 専門性に基づく責任分担と監視の多重化。
   - ライフサイクル全体でのセキュリティ設計。
5. 重要なポイント
   - Secure-by-Designと継続的監視が鍵。
   - インシデント対応プレイブックとSOC連携で迅速な封じ込め。

ご清聴ありがとうございました。

参考:

1. **ウィキペディア（2026）**
『デジタルツイン（Digital twin）』ウィキペディア、アクセス日：2026年1月。
2. **Dr. Michael Grieves, John Vickers（2016）**
『デジタルツイン概念の起源（Origins of the Digital Twin Concept）』Digital Twin Institute、2016年8月。
3. **IBM（2026）**
『デジタルツインとは？（What is a digital twin?）』IBM、アクセス日：2026年1月。
4. **Hazal Şimşek（2023）**
『自動車産業のデジタルツインのユースケース トップ5：2023年版
（Top 5 Use Cases of Digital Twin in Automotive Industry in '23）』AI Multiple、2023年1月1日。
5. **Guodong Shao, Deogratias Kibira（2018）**
『デジタルマニュファクチャリング：デジタルサロゲートを実装する際の要件と課題
（Digital Manufacturing: Requirements and Challenges for Implementing Digital Surrogates）』
2018 Winter Simulation Conference、2018年12月。
6. **Tomas Kulik, Cláudio Gomes, Hugo Daniel Macedo, Stefan Hallerstede, Peter Gorm Larsen（2022）**
『セキュアなデジタルツインを目指して（Towards Secure Digital Twins）』LNCS 第13704巻、2022年10月17日。
7. **David Holmes, Maria Papathanasaki, Leandros Maglaras, Mohomed Amine Ferrag, Surya Nepal, Helge Janicke（2021）**
『デジタルツインとサイバーセキュリティ – ソリューションなのか？課題なのか？
（Digital Twins and Cyber Security – solution or challenge?）』SEEDA 2021、2021年8月。

参考:

8. **瀬野 恕（2025）**
『自動車産業におけるデジタルツイン活用事例！導入効果、活用領域を紹介』メタバース、2025年11月。
9. **小宮昌人（2020）**
『デジタルツイン革命とポストコロナ時代の日本企業のオペレーション』知的資産創造、2020年9月号。
10. **NECソリューションイノベータ（発行年不明）**
『CASEとは？自動車業界で期待される技術革新とその影響』NECソリューションイノベータ。