層	脅威	説明
知覚／センシング（Perception / Sensing）	センサーのスプーフィング（GPS、LiDAR）	攻撃者が偽の GPS または LiDAR 信号を送信し、デバイスに誤った位置情報や存在しない物体を認識させ、誤ったナビゲーションや衝突回避判断を誘発します。
	カメラのブラインディング（レーザー攻撃）	高出力レーザー光を照射してイメージセンサーを飽和させ、白飛びや画素欠損を引き起こし、ビジョンシステムを実質的に機能不全にします。
	音声スプーフィング（超音波コマンド）	人間には聞こえない超音波トーンを悪用して、隠れた音声コマンドを発動させ、意図しない動作をエージェントに実行させます。
	センサーデータの改ざん	改ざんされたファームウェアが生のセンサー値（例：距離データのスケーリング）を操作し、上位層に誤ったデータを渡すことで推論を誤らせます。
	サイドチャネル攻撃	電磁波や電力消費の変動を盗聴することで、カメラの映像などプライベートなセンサーデータを再構成する可能性があります。
	リプレイ攻撃	以前記録された「安全な」センサー入力を再注入し、環境が変化してもデバイスが状況を誤認するようにします。
	無線妨害（RF ジャミング）	広帯域ノイズでレーダーや Wi-Fi などの無線センサー通信を妨害し、システムをフェイルセーフや低機能モードに追い込みます。
	磁場操作	外部の磁石やコイルで磁力計／IMU の値を歪め、SLAM やナビゲーションシステムの方位推定を破壊します。
エッジ認知（Edge Cognition）	モデル汚染攻撃	OTA 更新経路を悪用してオンデバイスの AI モデルをすり替え、特定の物体を無視するなど挙動を操作します。
	ファームウェア脆弱性の悪用	カーネルや RTOS（リアルタイム OS）の脆弱性を突いてルート権限で不正コードを実行し、AI パイプラインや保存データを完全に掌握します。
	敵対的機械学習（ML）入力	特殊に加工された物体（例：標識に貼られたステッカー）によって視覚モデルを誤認させ、危険な運転判断を引き起こします。
	敵対的サンプル	偽造された音声や映像を用いて顔認証や音声認識を欺き、虚偽の本人確認を通過させます。
	実行環境の脆弱性	AI ランタイム（TensorRT や ONNX など）のバッファオーバーフローや権限昇格の欠陥を突き、サンドボックスを脱出して推論処理を改ざんします。
	モデル抽出攻撃	API 呼び出しや処理時間の観測を繰り返し、オンデバイスの AI モデルを模倣して知的財産を盗用したり、特化型攻撃を準備したりします。
	サービス拒否（DoS）	CPU や GPU に無意味な推論リクエストを大量送信し、制御ループを飢餓状態にして遅延や安全停止を引き起こします。
クラウド認知（Cloud Cognition）	クラウドデータ侵害	テレメトリや映像を集約するクラウドサーバが侵害され、ユーザ環境やモデル資産が流出します。
	悪意あるモデル更新	サプライチェーン攻撃により更新チャネルが乗っ取られ、改ざん済みのモデル重みが大量のデバイスに配信され、即座にバックドアが挿入されます。
	クラウドサービスへの DDoS 攻撃	DDoS によりオーケストレーション基盤が停止し、クラウド API に依存するデバイスが機能を喪失します。

	学習データ汚染	攻撃者が悪意あるデータをクラウドの学習パイプライン（例：フェデレーテッドラーニング）に注入し、将来のモデルを危険な方向に誘導します。
	クラウドメタデータの悪用	設定ミスのあるストレージ、ログ、または IAM ロールを通じて、デバイスの認証情報やネットワーク構成が漏洩し、横方向の侵入に悪用されます。
	クラウド側サイドチャネル攻撃	同一物理 GPU 上に共存する仮想マシンがキャッシュや電力消費パターンを監視し、モデルパラメータやユーザデータを推測します。
学習／適応（Learning / Adaptation）	フェデレーテッドラーニング汚染	悪意のあるデバイス群が改ざん済みデータを送信し、統合モデル全体に攻撃者が意図する挙動を埋め込みます。
	不正なモデル改変	微調整済みのモデル重みを密かに書き換え、性能を劣化させたり、隠れたトリガーを埋め込みます。
	ローカルモデル更新の乗っ取り	中間者攻撃（MiTM）によって正規の更新ファイルがすり替えられ、デバイス検証前に悪意ある更新が適用されます。
	ビザンチン攻撃	協調する複数の不正ノードが矛盾した更新を送信し、集合学習を不安定化させたり遅延させたりします。
	メンバーシップ推論攻撃	攻撃者が適応モデルを照会して、特定の個人データが学習に使用されたかを推測し、個人情報を漏洩させます。
	モデル反転攻撃	勾配やロジット値を解析して、学習データ（個人画像やセンサーデータなど）を再構成し、非公開情報や機密情報を流出させます。
	異常検知の回避	攻撃トラフィックを学習済みの閾値以下に調整し、検知されずにモデルを徐々に汚染します。
行動／アクチュエーション（Action / Actuation）	不正な遠隔コマンド（ロボットの乗っ取り）	資格情報の窃取やプロトコルの欠陥を突いて、攻撃者が遠隔でロボットを操作・操縦・再配置します。
	悪意あるアクチュエータ指令	不正な経路データを注入して、ロボットアームを安全範囲を超える速度やトルクで動作させ、人身事故や機器損傷を引き起こします。
	物理的改ざん	配線の切断、シムボードの挿入、DIP スイッチの操作によって電子的な安全機構を回避し、アクチュエータ応答を改変します。
	制御チャネルの乗っ取り	CAN、UART、PWM などの通信ラインを傍受・上書きし、正規制御パケットを無効化して攻撃者の指令を優先させます。
	アクチュエータのキャリブレーション攻撃	校正値をわずかに改変し、動作位置のドリフトを発生させ、精度低下や隠れた安全リスクを生じさせます。
	タイミング攻撃	制御ループの競合状態を突くタイミングで信号を注入し、デバイスを不安定に動作させたり、重要な瞬間に停止させたりします。