IoT技術を活用したコネクテッドカーソリューション

人と自動車が調和する豊かなクルマ社会の実現に向け，自動車から収集される情報をクラウドで収集・分析し，新しい価値やビジネスを創出するための基盤として，コネクテッドカーが期待されている。その実現には，クラウドと接続する信頼性の高い通信システム，膨大なデータの解析技術が必要となる。
日立では,これまで情報通信分野で培ってきたIoT技術と自動車システム技術を融合したセンターサービスと車載機器を開発している。本稿では，コネクテッドカーを実現するキー技術を紹介する。

櫻井 康平 | Sakurai Kohei
片岡 幹雄 | Kataoka Mikio
小高 浩 | Kodaka Hiroshi
加藤 淳 | Kato Atsushi
寺岡 秀敏 | Teraoka Hidetoshi
木山 昇 | Kiyama Noboru

1. はじめに

インターネットを介して常時データセンターやインフラにつながるコネクテッドカーは，より安全で快適なサービスを提供できる次世代自動車として注目されている。自動運転をはじめとする高度な運転支援システムの基盤でもあるコネクテッドカーには高い情報処理性能や信頼性が求められる。

日立では，多様な製品分野で培った情報通信技術と自動車システム技術を融合し，コネクテッドカーを実現するプラットフォームとして，さまざまなセンターサービスと車載機器を開発している。

本稿では，コネクテッドシステムの動向と技術課題を概説し,キー技術である無線活用ソフトウェア更新技術,情報を守るセキュリティ技術，および，車載エッジコンピューティング技術について詳述する。

2. コネクテッドシステムの動向

2000年代のコネクテッドカー向けサービスは，渋滞情報配信などに代表されるデータ分析技術を活用したものが主流であった。サービス開始当初は，タクシーなどの商用車に対して，携帯通信網に接続可能な通信モジュールであるTCU（Telematics Control Unit）が搭載されていた。近年ではサービスの利便性向上により，自動車メーカーは乗用車へのTCU標準搭載を推進し，一般ドライバー向けにコネクテッドカーサービスを提供している。

さらに，自動車のインターネット接続が普及するにつれて，例えば，SNS（Social Networking Service）情報を取得してナビ画面上に表示するインフォテインメントサービスが普及してきた。また，リモートドアアンロックなど，センターから自動車に指令情報を配信すること

で，限定的ではあるが自動車の遠隔操作を可能とするサービスも登場してきた。今後さらにセンターと自動車が密に連携し，さまざまなサービスでセンターの分析結果を自動車制御にフィードバックすることが一般的になると考えられる（**図1**左参照）。フィードバック型サービスの実現においてセキュリティは重要な技術であり，日立では車載セキュリティの機能を担うゲートウェイの開発も推進している。

将来的に自動車とセンターは，同図右に示すシステムアーキテクチャとなるものと考えている。日立では，このシステムを実現する基盤技術の開発に取り組んでいる。センターには日立のIoT（Internet of Things）プラットフォームであるLumadaを活用している。

次章以降では，コネクテッドカーソリューションを支えるプラットフォームの実現に必要不可欠な，「OTA（Over the Air）ソフトウェア更新技術」，「セキュリティ技術」，「車載エッジコンピューティング技術」について，その詳細を紹介する。

3. OTAによる制御ソフトウェア更新

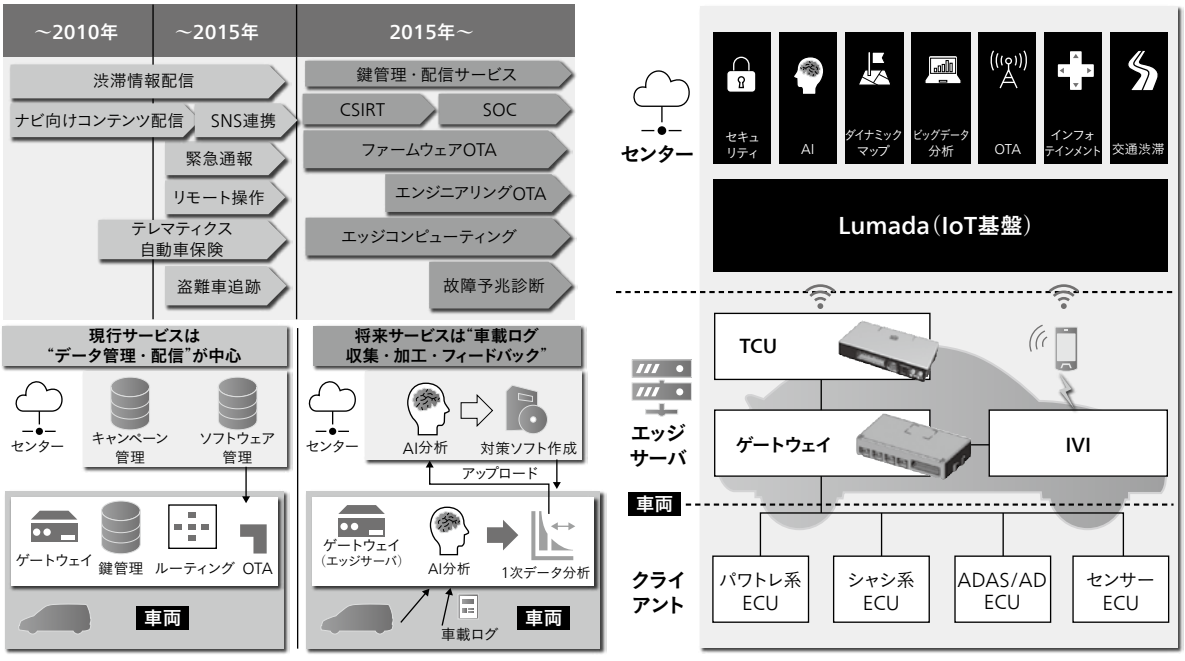
3.1 背景と課題

近年，自動車の制御がハードウェア中心からソフトウェア中心に移行し，車載ECU（Electronic Control Unit）に搭載されるソフトウェアの重要性が高まっている。ソフトウェアが制御の中心となることで，販売後の機能追加が可能になるなど，従来の自動車業界にはなかった新たな価値が生み出される一方で，ソフトウェアに起因するリコールが増大する懸念がある。また，コネクテッドカーの増加に伴い，遠隔からの攻撃などの，セキュリティリスクの増大が懸念されている。このような環境変化に対応するための技術として，無線を活用したOTAによる制御ソフトウェア更新技術が注目されている。

自動車にOTAを適用するためには，ソフトウェア更新処理による安全への影響や更新失敗などによる車両不稼働を回避する高い信頼性が必要となる。ユーザーが車

図1｜コネクテッドカーサービスのロードマップとシステムアーキテクチャ

データ分析と単純な情報配信のサービスから，分析結果をフィードバックするサービスに変化していく様子を左に，エッジコンピューティングにおけるエッジサーバ機能を，TCU，ゲートウェイ，IVIが担っている様子を右に示す。



注：略語説明
SNS（Social Networking Service），CSIRT（Computer Security Incident Response Team），SOC（Security Operation Center），AI（Artificial Intelligence），OTA（Over the Air），TCU（Telematics Control Unit），IoT（Internet of Things），IVI（In-vehicle Infotainment），ECU（Electronic Control Unit），ADAS（Advanced Driver Assistance System），AD（Autonomous Driving）

両を使えない時間をできるだけ短くするとともに，バッテリーの消費を抑えるための更新時間の短縮や，異なる振る舞いをする多数のECUから構成される複雑で多様なシステムへの対応が特に重要である。

3.2 日立のOTAソフトウェア更新技術

日立では，前述の主要課題を解決し，自動車システムへのOTA適用を可能にする以下の技術を開発した（**図2**参照）[1), 2)]。

・ネットワーク帯域やメモリリソースに制約のある自動車システム環境下で更新時間を短縮する差分更新技術

・安全要件やメモリリソースなどのECU仕様やコスト要件に合わせた更新異常時のリカバリー技術

・センターから車両への更新データ配信を多層で防御するEnd to Endセキュア配信技術

・車種やECUの相違による更新手順の違いに柔軟に対応可能な更新制御技術

・センター・車両間，車両内のECU間のインタフェースに標準技術を適用するとともに，複数サプライヤーのECU更新データをパッケージ化して配信するマルチサプライヤー対応技術

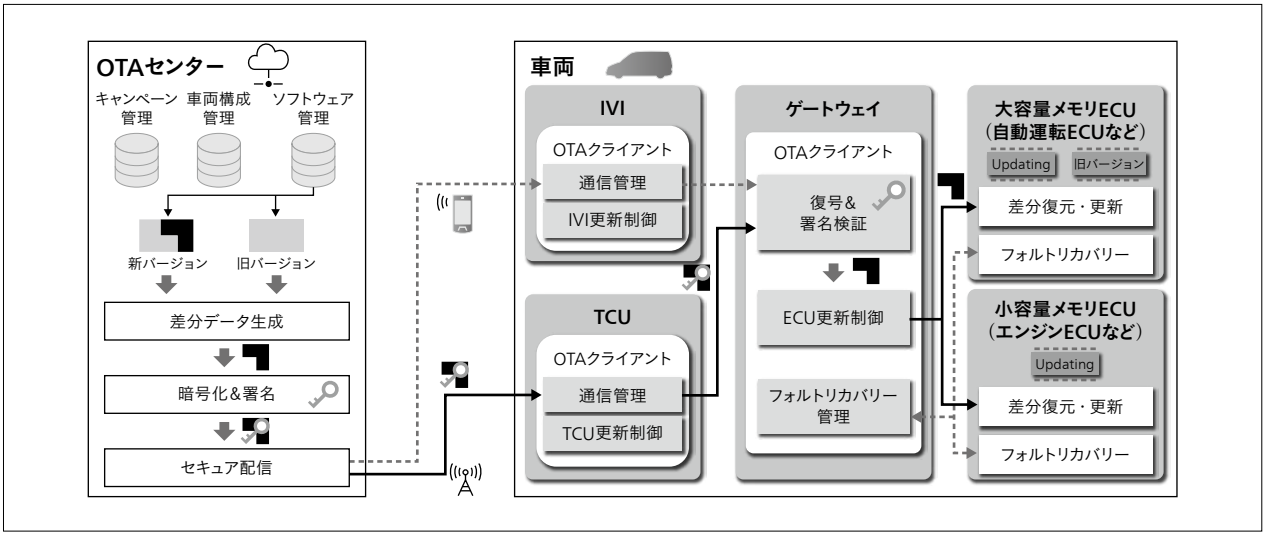
日立では，これらの技術を搭載したTCU，ゲートウェイ，ECU，および，センターシステムを開発した。これらの部品，システムから成るOTAソリューションをワンストップで提供していく。

3.3 今後の展開

ソフトウェア更新は，市場に出た自動車だけでなく，

図2｜OTAシステム構成

センターシステムから更新対象ECUまでのトータルシステムを構築し，システム視点で各機能の要件を抽出した。機能安全・セキュリティ確保のため，制御ECUの更新制御機能はゲートウェイに搭載した。センター・車両間および車両内のECU間のインタフェースには標準技術を適用し，マルチサプライヤーでのシステム構築が可能である。



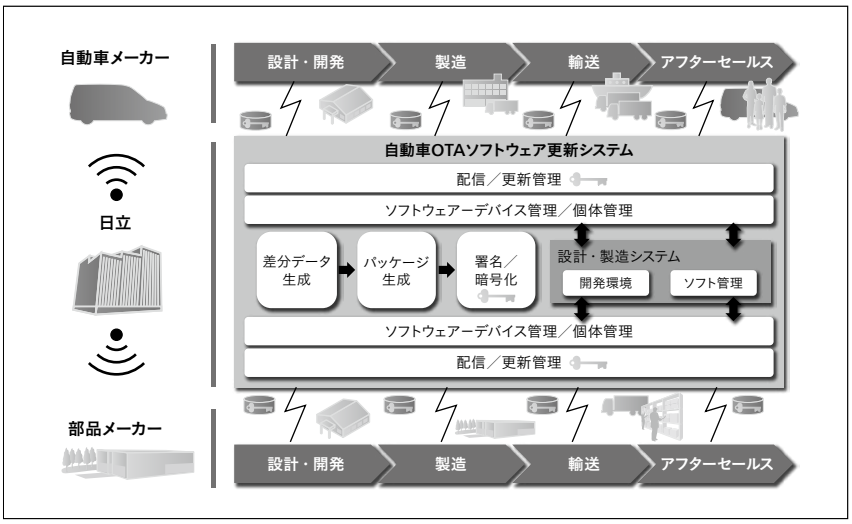


図3｜開発工程および製造工程でのOTA

アフターセールスと同様，開発工程や製造工程でもソフトウェア書き込みの無線化により業務効率向上に貢献できる。

自動車メーカーの開発工程，製造工程（製造ライン），輸送工程（港や自動車保管場），および，部品メーカーの製造工程，輸送・保管工程にある部品への対応も必要となる。

今後は，PLM（Product Lifecycle Management），MES（Manufacturing Execution System）と，OTAソフトウェア更新システムの車両個体管理，ソフトウェア－デバイス管理を連携させることで，ライフサイクル全体でソフトウェア更新・管理業務の効率化，リコール対策の効率化，トレーサビリティ向上をめざす（**図3**参照）。

4. セキュリティ技術

4.1 背景と課題

自動車のコネクテッド化により，これまで車両内に閉じていたネットワークがインターネットなどの外部ネットワークに接続される。このため，外部ネットワークから車両への攻撃が懸念され，遠隔での不正操作や，車両・センター間通信情報の盗み見などのセキュリティリスクをいかに低減するかが課題となる。

日立は，ゲートウェイを次世代自動車のキーコンポーネントと位置づける。ゲートウェイは，車両内の異なるネットワーク間での相互通信を可能とするルーティング機能に加え，車両内の通信を監視しセキュリティを確保する車載通信セキュリティ機能，および，ライフサイクルを通じて車両の品質とセキュリティを向上するセンター連携セキュリティ機能を備える。

4.2 車載通信セキュリティ機能

ゲートウェイには，車両の脅威分析結果から抽出された車両内外の脅威から車両を守るため，以下のセキュリティ機能を搭載する。これらのセキュリティ機能により，ゲートウェイは車両外部からの攻撃の内部ネットワークへの侵入を防止する。

・不正な通信のフィルタリング
・不正なソフトウェア書き換えを検知するセキュアブート
・不正な機器の接続を防ぐ機器認証
・メッセージ正当性確認のためのメッセージ認証
・DoS（Denial of Service）攻撃対策

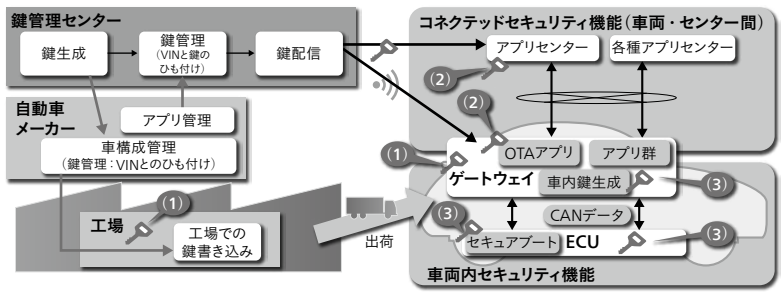
4.3 センター連携セキュリティ機能

セキュリティでは，現在想定される攻撃への対策だけではなく，常に高度化していく攻撃手法への対策も必要となる。そのため，開発時のセキュリティ対策だけではなく，運用時に車両の状態を監視し，迅速な対処を実施することが求められる。

自動車のライフサイクル全体でセキュリティを維持するためのセンター連携セキュリティソリューションを以下に示す。

(1) 鍵管理ソリューション

セキュリティ技術の実現には，センターと車両間，および，車両内のECU間で，互いの真正性確認と通信路保護に利用する暗号鍵の管理が必要であり，車両の製造時から廃棄までのライフサイクルにわたる鍵管理ソリューションを提供する（**図4**参照）[3)]。



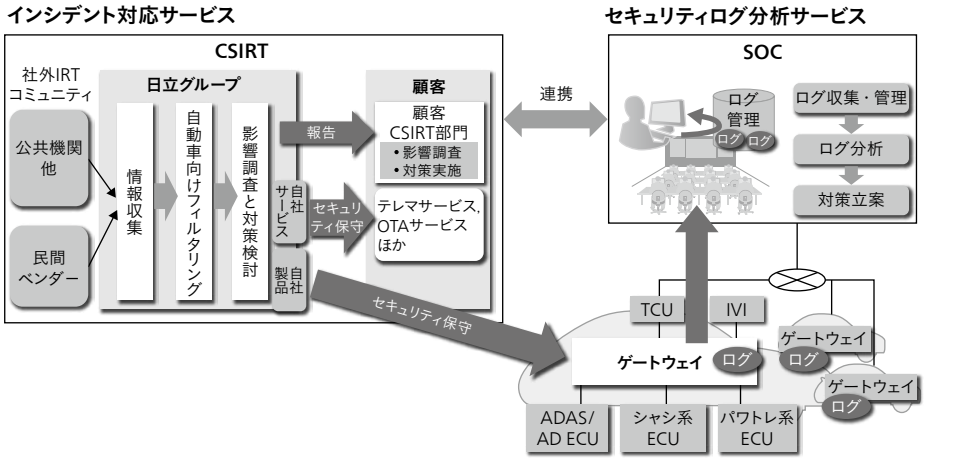
鍵の種類	内容
(1)ベース鍵	(1)車のセキュリティを担保するための基盤となる鍵（トラストアンカー） 鍵管理センターで生成して工場で書き込む。
(2)アプリ鍵	(2)センターとゲートウェイ間のデータを送受し，機器認証と，データの暗号化・復号をする鍵 ベース鍵を用いて鍵管理センターからサービスセンター，ゲートウェイへ配信する（定期的に更新）。
(3)車内鍵	(3)車内ネットワーク／ECUで，ECU間認証，メッセージ認証，セキュアブートに使用する鍵 ゲートウェイ内でベース鍵をもとに生成し，車両内のECUへ配信する（定期的に更新）。

注：略語説明
VIN（Vehicle Identification Number），CAN（Controller Area Network）

図4｜鍵管理ソリューション
車両の製造から利用まで全体を見据え，コネクテッドサービス，車両内のECU間の認証，暗号化で必要な「鍵の生成から運用まで」を実現する鍵管理ソリューションを提供する。

図5｜セキュリティサービスソリューション

インシデント情報収集・分析による事前対策と，ログ分析による攻撃の早期発見・対処により，常に高度化するセキュリティ攻撃を防ぐ。



注：略語説明
IRT（Incident Response Team）

(2) セキュリティサービスソリューション

日立は情報系システムで培った技術により，ゲートウェイで検知した攻撃に関するログ情報をセンター側で収集・分析し，以下のような対策案を自動車メーカーに迅速に提供する（**図5**参照）。

・インシデント対応サービス

攻撃の早期認識，対策の実施により自動車のセキュリティを守る運用を実現するため，製品・サービスに関わる脆（ぜい）弱性・インシデントを収集し，自動車メーカーに提供する。

・セキュリティログ分析サービス

インシデントの影響を最小限に抑え，早期復旧を実現するため，自動車のログを収集･分析し，自動車メーカーのセキュリティ脅威の原因分析と対策立案を支援する。

5. 車載エッジコンピューティング技術

4.3で記述したセキュリティログ分析サービスに代表されるように，今後，1台の自動車から収集するデータは肥大化していくと考えられる。さらに，コネクテッドカーが増加すると，データ通信量の増大が課題になる。この背景から，今後のコネクテッドカーを実現するプラットフォームには，以下のようなデータ量削減の機能が必要になると考えられる。

・通常時は，限定的なセンサー／ログ情報を低頻度で車載機器から収集し，センターに送信する。

・異常時や，センターから指示があった場合に限り，多数のセンサー／ログ情報を，高頻度で車載機器から収集し，センターに送信する。

これらはIoT分野におけるエッジコンピューティング技術と同等であり，サービスの品質を確保しながら，車両から収集するデータ量を低減させることができる。

このようなデータ収集ルールに従って統計加工処理を施す機能は，さまざまなECUのセンサー／ログデータが集まるゲートウェイに搭載する。一方で，組み込み機器であるゲートウェイは，セキュリティ機能やルーティング機能などの他機能も担うため，CPU（Central Processing Unit）・メモリなどのリソースの余力は十分ではない。そこで日立では，リソース制約のあるハードウェアでも実行可能な車載向けエッジコンピューティング技術を開発した（**図6**参照）。

この技術では，車載機器におけるルール変更の実装方式として，スクリプト言語とコンパイラ言語を併用することで車載機器のリソース消費量を低減する。一般的に，スクリプト言語はコンパイル不要でありプログラムの変更容易性が高いが，実行にはCPU／メモリなどのリソース消費量が大きい。一方で，コンパイル言語はスクリプト言語と比較してリソース消費量は小さいが，プログラム変更にはコンパイル処理が必要なため，変更容易性が低い。そこで，以下の2つの言語で実装することで，変更容易性とリソース消費量低減を両立している。

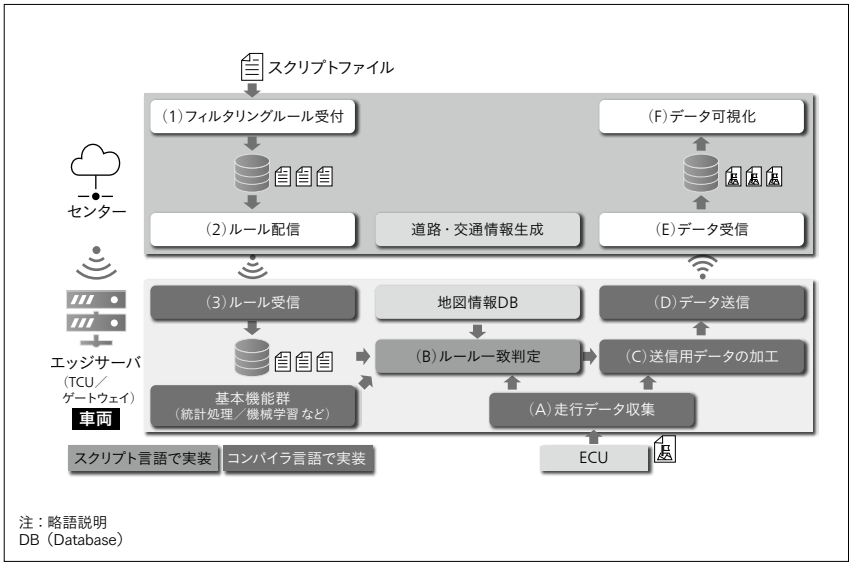
(1)機械学習や統計処理など，変更する頻度は少ないが，リソース消費量の大きい処理はコンパイラ言語

(2) 比較演算や関数呼び出しなど，変更する頻度は多いが，リソース消費量の小さい処理はスクリプト言語

ルールを変更したい場合には，新しいルールを記述したスクリプトファイルをセンターからゲートウェイに配信することで，ゲートウェイはスクリプトファイルを上書きし，即座に新しいルールを適用できる。

図6｜スクリプト配信型エッジコンピューティング基盤

基本的な統計処理機能を低負荷なコンパイラ言語で実装し，その統計処理機能の組み合わせをスクリプト言語で制御する方式とすることで，プログラム変更の容易性と処理負荷低減を両立した。



注：略語説明
DB（Database）

6. おわりに

本稿では，日立で開発しているコネクテッドカー向けプラットフォーム技術について述べた。

日立はTCU，ゲートウェイなどの車載機器や，OTAソフトウェア更新，セキュリティなどのセンターサービス，さらには，車両側で大量の情報を一次処理するコンピューティング技術を組み合わせたソリューションを提供し，より安全，快適で人とクルマが調和する豊かなスマートモビリティ社会の実現に貢献していく。

参考文献

1) 寺岡秀敏，外：車載ECU向け差分更新方式，情報処理学会論文誌コンシューマ・デバイス＆システム（CDS），7（2），41～50（2017.5）
2) H. Teraoka et al.: Incremental update method for resource-constrained in-vehicle ECUs, IEEE 5th Global Conference on Consumer Electronics（2016）
3) 森田伸義，外：車載システム向けセキュリティ分析支援ツールの提案，暗号と情報セキュリティシンポジウム（SCIS）（2014）

執筆者紹介

櫻井 康平
日立オートモティブシステムズ株式会社
情報安全システム事業部 設計開発本部
情報通信設計部 所属
現在，車載情報安全システム製品の量産開発業務に従事
博士（情報科学）
自動車技術会会員，日本物理学会会員

片岡 幹雄
日立オートモティブシステムズ株式会社
情報安全システム事業部 設計開発本部
情報通信設計部 所属
現在，車載セキュリティ技術の設計開発に従事
自動車技術会会員，電子情報通信学会会員

小高 浩
クラリオン株式会社
セーフティアンドインフォメーションシステム事業推進本部
セーフティアンドインフォメーションシステム情報通信開発部 所属
現在，TCUの製品開発に従事

加藤 淳
日立製作所 産業・流通ビジネスユニット
産業ソリューション事業部
モビリティ＆マニュファクチャリング本部 所属
現在，コネクテッドカーサービスの企画・開発に従事

寺岡 秀敏
日立製作所 研究開発グループ システムイノベーションセンタ
システム生産性研究部 所属
現在，車載システムの研究開発に従事
情報処理学会会員

木山 昇
日立製作所 研究開発グループ
東京社会イノベーション協創センタ 顧客協創プロジェクト 所属
現在，コネクテッドカーサービスの研究開発に従事
博士（情報科学）
情報処理学会会員