特集論文

車載マルチメディアヘッドユニット向けインターネット経由ソフトウェア更新機能

太田浩祐*

Flexible Software Update via OTA for Car Infotainment Head Unit

Kosuke Ota

要　旨

車両に搭載されるカーマルチメディア機器(Infotainment Head Unit：IHU)向けにOTA(Over The Air)機能を開発した。OTAとは，インターネット経由でユーザー自身がソフトウェアなどのコンテンツを更新できる機能である。既に携帯電話・スマートフォンでは一般的になっているこのOTA機能を，今回，車載機器にも搭載した。従来，車載機器のソフトウェアを更新するには，ユーザーがディーラーに車両を持ち込んでディーラーが作業する必要があった。この機能を搭載することでユーザー自身によるソフトウェアの更新が可能になった結果，ソフトウェア更新作業の費用削減や更新ソフトウェアの迅速な市場投入が期待できるようになった。

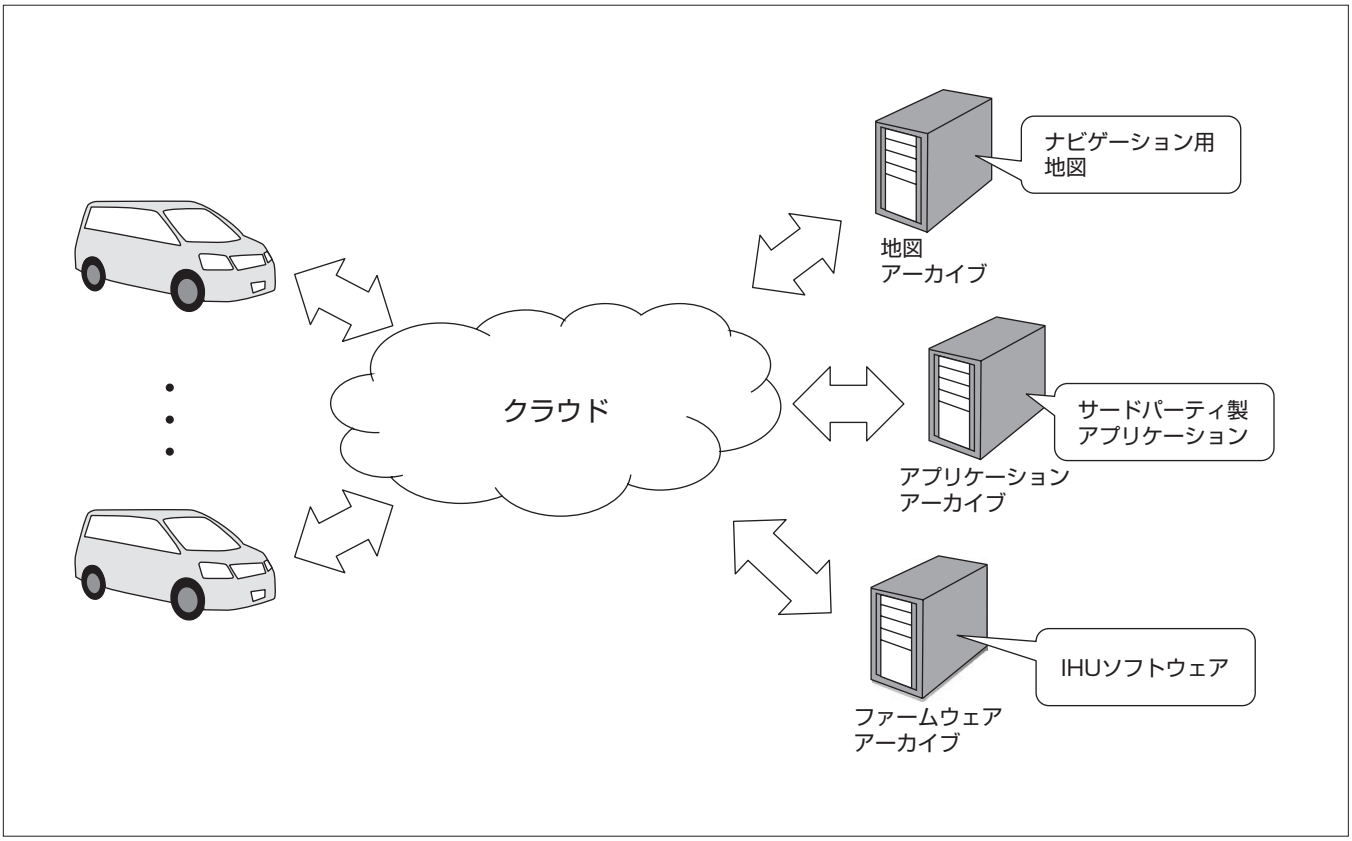
その一方で，車載機器のソフトウェア更新に対して，不特定多数のユーザーが関与可能となるので，従来のOTAへの対応に加えて次の課題への対応も必要となった。

(1)　ソフトウェア更新による走行中のIHU機能停止の防止

(2)　動作保証されていない組合せのソフトウェア更新の防止

(3)　第三者によるソフトウェアの改ざん対策

これらの課題を解決して，車載機器に対して便利かつ安全なソフトウェア更新機能を開発できた。今後，この機能を利用したIHUの新規サービス(機能)の投入増加が予想され，この機能の重要性はますます高まる見込みである。ユーザーニーズ，技術動向によって検討すべき課題は変化していくが，継続的にこの機能の改善・向上を図ることでユーザーニーズに適合したサービスを提供していく。



OTA機能の全体構成

OTA機能の概念図である。自動車メーカーが準備したクラウド／サーバと各車両が無線通信することで，OTA機能を実現している。今回開発したOTA機能では，ナビゲーション用地図，サードパーティ製アプリケーション及びIHUのソフトウェアを更新することができる。

*三田製作所

1. まえがき

車両に搭載されるIHU向けにOTA機能を開発した。この機能は，無線通信によるインターネット接続を用いてナビゲーション用地図，サードパーティ製アプリケーション及びIHUのソフトウェアの更新を可能にする。この機能を搭載したことで，次の効果が期待できる。

(1) ソフトウェア更新の費用削減
(2) 更新ソフトウェアの迅速な市場投入

従来，ソフトウェアを更新する際には，ユーザーがディーラーまで出向いて，ディーラーの作業で1台ずつソフトウェアを更新する必要があった。また，新サービスの追加によるソフトウェアの更新が生じた際でも更新できるタイミングが限られており，すぐに新しいソフトウェアを提供することができなかった。

しかし，OTA機能を搭載することでユーザー及びディーラーの手間を省き，かつ，新サービスの迅速な投入が可能となる。

本稿では，OTA機能の基本的な仕組み，及びOTA機能の実現に向けた課題と対策を述べる。

2. OTA機能

OTA機能は大きく分けて次の2つの機能で実現している(**図1**)。

(1) ダウンロード(クラウドからのデータのコピー)
(2) インストール(ソフトウェアの書換え)

基本機能には信頼のある既存ソフトウェアを活用し，車載特有の課題解決に注力した。それぞれの機能について，次に述べる。

2.1 ダウンロード

ダウンロードは，クラウドに格納されているソフトウェアをIHUの一時領域にコピーする。今回開発したOTA機能では，クラウドとの通信をIHUとは別の通信ECU(Electronic Control Unit)で実現しており，ソフトウェアのコピーもこの通信ECUで実現している。ユーザーの画面操作で通信ECUがソフトウェアのダウンロードを開始する。通信ECUはIHU内の一時領域にアクセスして，コピーしたソフトウェアを格納する(**図2**)。

2.2 インストール

インストールは，一時領域に格納したソフトウェアを実行領域に書き込む。今回開発したシステムでは，OTA機能以外にもUSB(Universal Serial Bus)メモリによる更新，Ethernet(注1)経由での専用ツールによる更新が可能である(**図3**)。OTA機能のインストールは，これらの更新機能を流用して開発した。インストールの仕組みを統一することで，後に述べる課題の解決にも効果を発揮した。

(注1) Ethernetは，富士ゼロックス㈱の登録商標である。

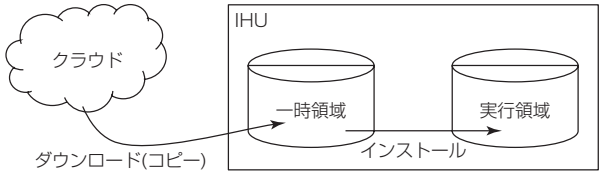


図1．OTAの基本的な仕組み

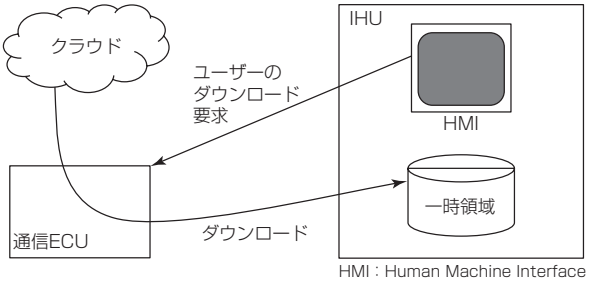


図2．ダウンロードの方法

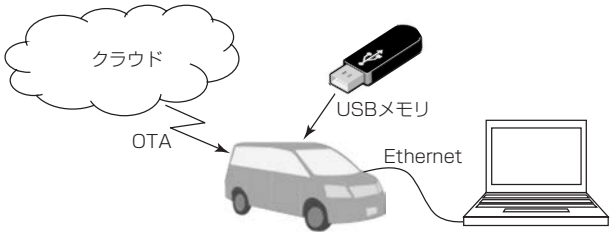


図3．ソフトウェア更新の3つの手段

3. 車載用OTAで実現した機能

ユーザー自身によるソフトウェア更新を可能にするOTA機能を安全に提供するために，次の課題の解決を図った。

(1) ソフトウェア更新による走行中の機能停止防止
(2) ソフトウェア更新中のシャットダウン対策
(3) 動作保証されていない組合せのソフトウェア更新の防止
(4) ソフトウェア更新の競合対策
(5) 第三者によるソフトウェアの改ざん対策

それぞれの課題の解決策を，項目順に述べる。

3.1 実行領域の2面持ち

ユーザーが走行中にOTA機能を作動させることを想定して，IHUの通常動作中に並行してソフトウェアの更新を実行できる必要がある。しかし，IHUには車両の走行に密接に関連する機能も搭載されており，一時的であっても走行中のソフトウェア更新によるIHUの機能停止は許容されない。

この対策として，アプリケーション実行用と更新ソフトウェア書き込み用の2つの実行領域を用意することで，この課題を解決した(**図4**)。

図4の実行領域(A)でアプリケーションが実行されている状態でOTA機能によるソフトウェアの更新が要求された場合，更新ソフトウェアをソフトウェア書き込み用の実行領域(B)に書き込む。更新ソフトウェアの実行領域(B)への書き込みが完了するまで，アプリケーションは実行領域(A)で実行される。IHUが次に再起動するタイミングで

実行領域を切り換えて，新しくソフトウェアが書き込まれた実行領域(B)でアプリケーションを実行する。この対応によって，走行中にIHUの機能を損なうことなくソフトウェア更新することを実現できた。

また，ディーラーによるソフトウェア更新では走行中のソフトウェア更新を想定していないため，この対応は必ずしも必要ではなかったが，ソフトウェア更新の失敗時など不完全なソフトウェアでの実行による動作不具合を回避するために，この対策を適用した。

3.2 レジューム

先に述べたとおり，OTA機能はユーザーが走行中に実行することも想定している。そのため，他の機能の動作に影響を与えないようにOTA機能の処理優先度を下げる必要がある(バックグラウンドでソフトウェアを更新)。処理優先度を下げることで処理完了までに時間がかかり，ソフトウェア更新完了前にIHUがシャットダウンされる可能性が高まる。その際，ソフトウェア更新が中断されることで次回起動時に初めから更新が必要ということになれば，OTA機能のユーザビリティを著しく低下させる。

この対策として，レジューム機能を搭載して，シャットダウンによるソフトウェア更新の初めからのやり直しを回避した。レジューム機能とは，前回終了時に中断した箇所から処理を再開させる機能である(**図5**)。レジューム機能を搭載しない場合，前回終了時にどこまで処理したのかを判断できず，次の起動時に初めから処理を再開する必要があった。しかし，レジュームポイントを設定することで，シャットダウン前までにどのレジュームポイントまで処理したかを記憶して，前回終了時に中断したレジュームポイントからソフトウェア更新処理を再開できるようにした。

3.3 ソフトウェアの互換性チェック

IHUのソフトウェアは多数のソフトウェアモジュールで構成されており，様々なバージョンが存在するが，全てのバージョンの組合せによる動作保証は困難である。そのため，保証できないソフトウェアの組合せへの更新は避ける必要がある。

そこで，クラウドによる更新可能なソフトウェアの管理及びソフトウェア更新時のバージョンチェックを導入して，これらの課題を解決した。

それぞれの解決策の詳細を次に述べる。

(1) クラウドによる更新可能なソフトウェアの管理

動作保証されているソフトウェアのバージョンだけを，更新可能なソフトウェアとしてユーザーへ提供することで，動作保証されていない組合せのソフトウェアへの更新を防止する(**図6**)。

ユーザーがソフトウェア更新を実行すると，IHUは現状のソフトウェアバージョンをクラウドに通知する。クラウドは現状のソフトウェアバージョンを確認して，更新可能なソフトウェアのリストをIHUへ通知する。このように更新可能なソフトウェアだけを選択可能な形でユーザーへ提供することで，動作保証されていない組合せのソフトウェ

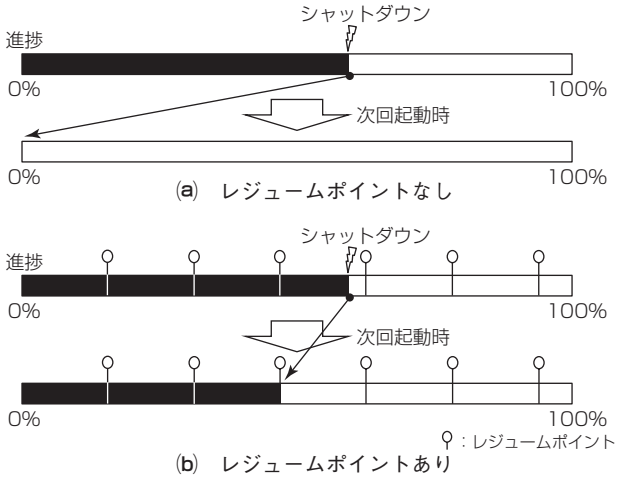


図5．レジュームポイント

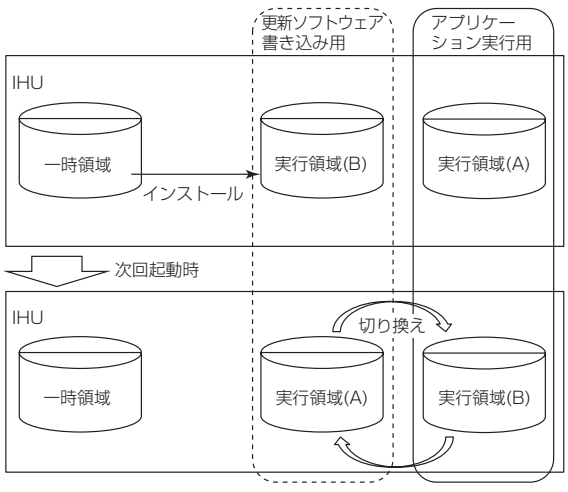


図4．実行領域の2面持ち

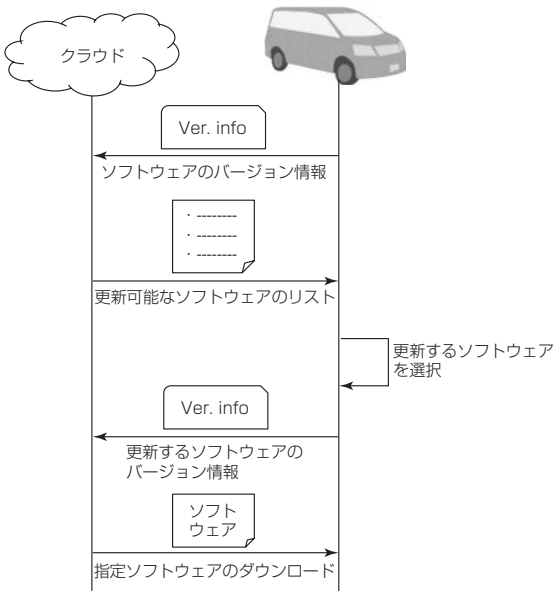


図6．ソフトウェアのバージョン管理

アへの更新を防止した。

⑵ ソフトウェア更新時のバージョンチェック

通常のソフトウェア更新の際，各ソフトウェアのバージョンチェックを実行する。IHU内に組み合わせ可能なソフトウェアのデータベースを保持しておき，更新予定のソフトウェアの組合せに問題がないかをこのデータベースで照合する。保証されていない組合せのソフトウェアが検出された場合は，そのソフトウェアの更新を中止する。しかし，この対応方法では，将来の更新ソフトウェアを考慮した場合に組合せが増大して管理が困難となることが予想される。この問題に対して次の方策を導入して，ソフトウェアの組合せ数を削減した。

確認する組合せのベースとなる更新頻度の高いソフトウェアを定義して，そのベースソフトウェアと更新頻度の低い他のソフトウェアとの組合せを確認することで組合せ数を削減した(この際，更新頻度の低いソフトウェア同士の組合せは確認しない)。なお，ベースソフトウェアではないソフトウェア間に依存関係がある場合は，そのいずれかをベースソフトウェア(サブ)として，階層化する必要がある(**図7**)。

このソフトウェアの組合せチェックは，OTA機能だけではなく他のソフトウェア更新にも適用することで，動作保証されていない組合せのソフトウェアの実行を回避した。

3.4 ソフトウェア更新の排他制御

複数の手段でのソフトウェア更新が可能であるため，異なるバージョンのソフトウェアが同時に書き込まれる可能性があり，異なる手段での同時ソフトウェア更新の防止が必要となる。

その対策として，ソフトウェアの更新権管理機能を導入した。この機能は，初めに選択された更新手段へソフトウェアの更新権を与えて，ソフトウェア更新が既に他の手段で実行されている場合は，後から選択された更新手段でのソフトウェア更新を禁止する。これによって，複数の手段で同時にソフトウェアが更新される事態を回避した。

3.5 ソフトウェアの改ざんチェック

第三者によって改ざんされたソフトウェアの更新で，IHUが意図しない動作に陥る可能性がある。各機種の構成によって検討すべきユースケースは異なるが，基本的には，ダウンロード時及びインストール時の対策が必要である。それぞれの対策を次に述べる。

⑴ ダウンロード時のチェック

OTA機能では，無線通信を用いてダウンロードを実施するため，クラウドからソフトウェアを受け取るまでの間にソフトウェアが改ざんされていないことを確認する必要がある。

この対策として，SSL(Secure Sockets Layer)／TLS(Transport Layer Security)による暗号化を採用することで，問題を回避した。この技術は，無線通信における一般的な技術である。

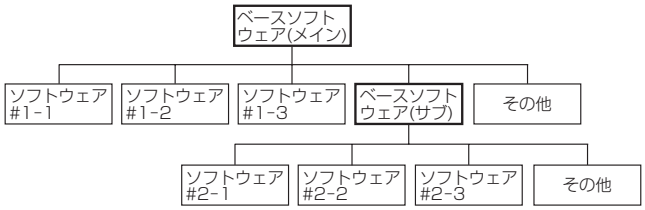


図7．組合せチェック

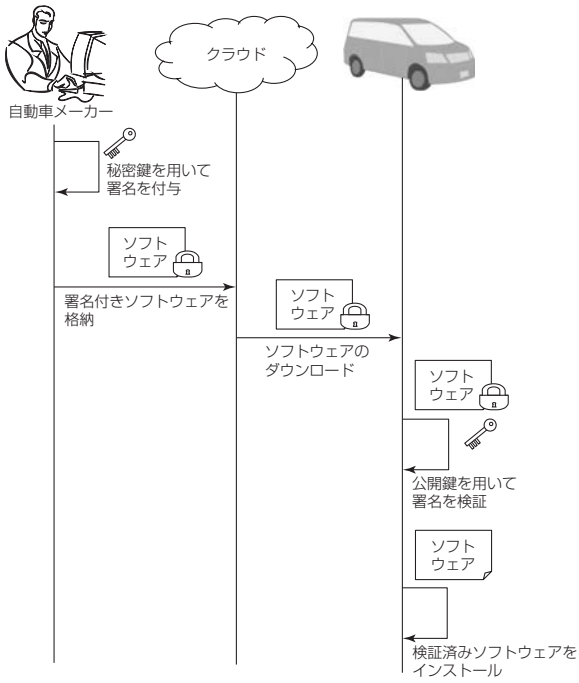


図8．署名付与フロー

⑵ インストール時のチェック

ダウンロード前，又はダウンロード後にソフトウェアが改ざんされた場合，先に述べたチェックだけでは不正ソフトウェアの更新を抑止しきれない。そのため，インストール前にソフトウェア改ざんの有無を検出する必要がある。

この対応として，署名付きソフトウェアに対する認証方式を導入した(**図8**)。クラウドに格納する各ソフトウェアに対して署名を付与する。IHUはソフトウェアのインストール前に付与されている署名を検証して，ソフトウェアが改ざんされていないことを確認する。

4. むすび

OTA機能を実現するために，ソフトウェア更新時のユーザー操作の検討に十分な配慮を必要とした。それらのユースケースを洗い出して1つ1つ検討していくことで，ユーザーにとって便利で安全なソフトウェアの更新機能を提供することができた。今後，この機能を利用したIHUの新規サービス(機能)の投入増加が予想され，この機能の重要性はますます高まる見込みである。ユーザーニーズ，技術動向によって検討すべき課題は変化していくが，継続的にこの機能の改善・向上を図ることでユーザーニーズに適合したサービスを提供していく。