公衆通信回線と情報セキュリティー技術を活用した車上データベースの更新


北野　隆康
Takayasu Kitano
信号技術研究部
列車制御システム研究室
主任研究員


久保田　淳司
Junji Kubota
前 信号技術研究部
列車制御システム研究室
副主任研究員


祇園　昭宏
Akihiro Gion
信号技術研究部
列車制御システム研究室
主任研究員


藤田　浩由
Hiroyuki Fujita
信号技術研究部
列車制御システム研究室長

はじめに

近年，車上装置にデータベースを搭載して活用することで，速度照査☞を実現する運転保安システムの導入が進んでいます。車上データベースに車両の性能や制限速度区間，地上設備の位置などの情報を登録していますが，線形変更などで登録情報に変更が生じると更新が必要となります。現状では係員が各車両にて更新作業を行っているため，多くの工期や人的リソースを要することが課題になっています。そこで，公衆通信回線を活用して車上データベースを更新する手法を確立するため，配信された更新データに対するセキュリティーと健全性を同時に検証する機能を開発しました。本手法を適用することで，車上データベース更新の省力化や自動化による生産性向上が可能となります。本記事では，本手法の開発のコンセプトと車上データベースの更新手順，および模擬装置にて実施した動作確認の結果について述べます。

車上データベースの概要

車上装置で連続的な速度照査パターンを発生させ，列車速度などを制御する運転保安システムでは，車上装置に搭載したデータベースに線路条件や地上設備などの情報を登録して，速度照査パターンの発生に活用しています。車上データベースは，一般に，車両性能データベースと線路データベースから構成されています。車両性能データベースには，車両最高速度，加減速度などの速度照査パターンの生成に必要な情報や位置検知に必要な情報などが登録されます。線路データベースには，位置情報（線区，区間，上下種別，区間長など），線区最高速度，制限速度（曲線，勾配，分岐など），現場機器の設置位置の情報などが登録されます（図1）。

車上データベース更新の課題

車上データベースは，線形変更などで分岐や地上子の位置が変更されるたびに線路データベースの登録情報を更新する必要があり，現在は，係員が車両基地に留置された車両内にて作業を行っています。例えば，外部記憶媒体を用いて車上装置に更新データを書き込む方法や，メーカーの工場内にてあらかじめ更新データを基板に書き込んで留置された車両内にて基板を交換する方法が採用されています（図2）。さ

☞ **速度照査**

安全を担保するために，車上で安全に走行できる速度を演算し，その速度と現在速度を比較することです。安全に走行できる速度を走行位置ごと連続的に表現した曲線を速度照査パターンと呼び，列車の速度が速度照査パターンを超過するとブレーキをかけます。

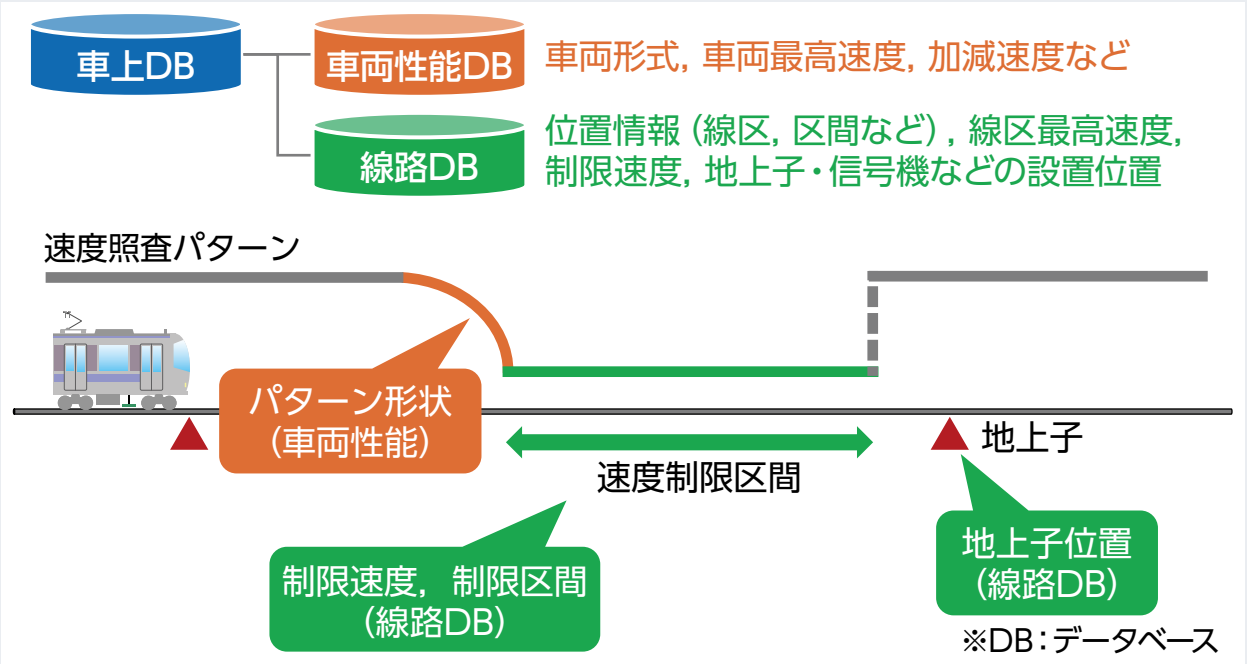

図1　車上データベースの概要

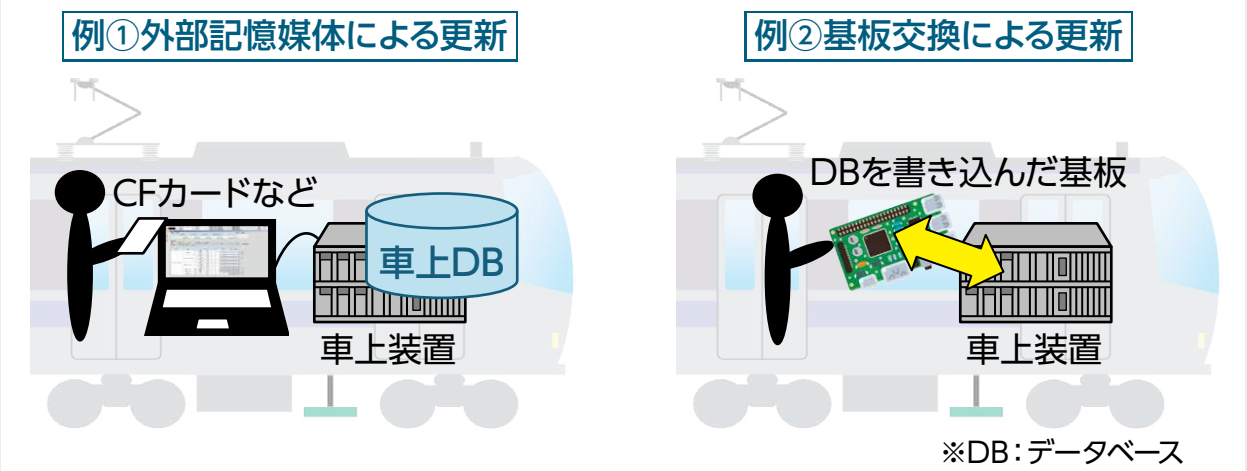

図2　車上データベース更新作業の例

らに，車上データベースを搭載する全ての車両に対して更新作業を実施する必要があるため，データ更新の作業時間の確保や車両の運用に関わる調整にも多くの人的コストと時間が必要となることが課題となっています。

公衆通信回線を活用した車上データベースの更新

車上データベース更新手法開発のコンセプト

車上データベース更新の課題を踏まえて以下のコンセプトを定め，公衆通信回線を活用した車上データベース更新手法（図3）を開発しました。

①作業の省力化：地上の中央装置に全データを集約して一元管理し，各車両に対して更新データを配信して自動的に車上データベースを更新することで，人的コストを削減する

②車上データベース更新の柔軟性：更新する場所や時間に制約されない手法により，車上データベース更新の柔軟性を確保する

③安全性とセキュリティーの確保：更新データの破壊や外部の第三者からの攻撃を想定し，暗号化技術により，配信した更新データの健全性を確保する

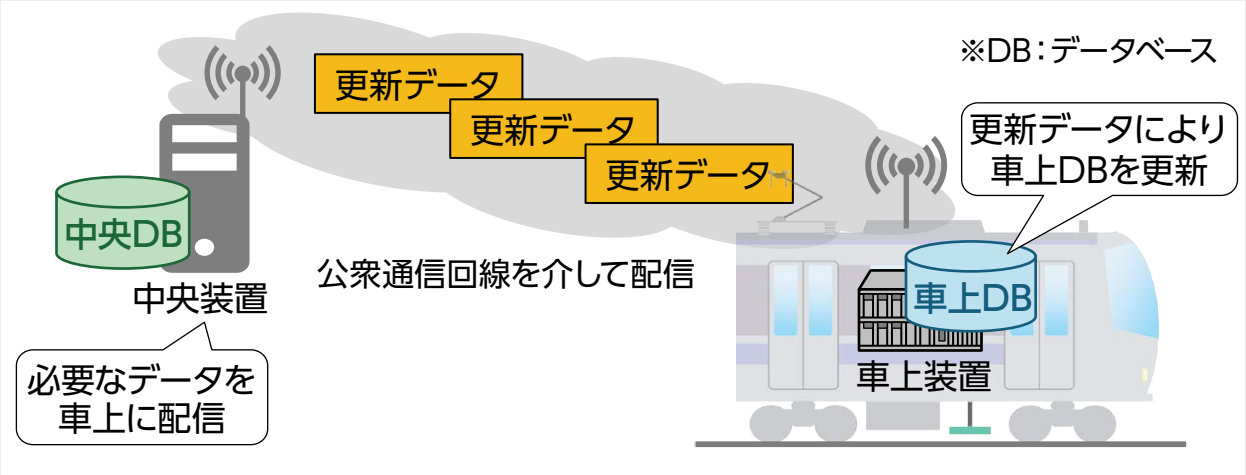

図3　公衆通信回線を活用した車上データベース更新

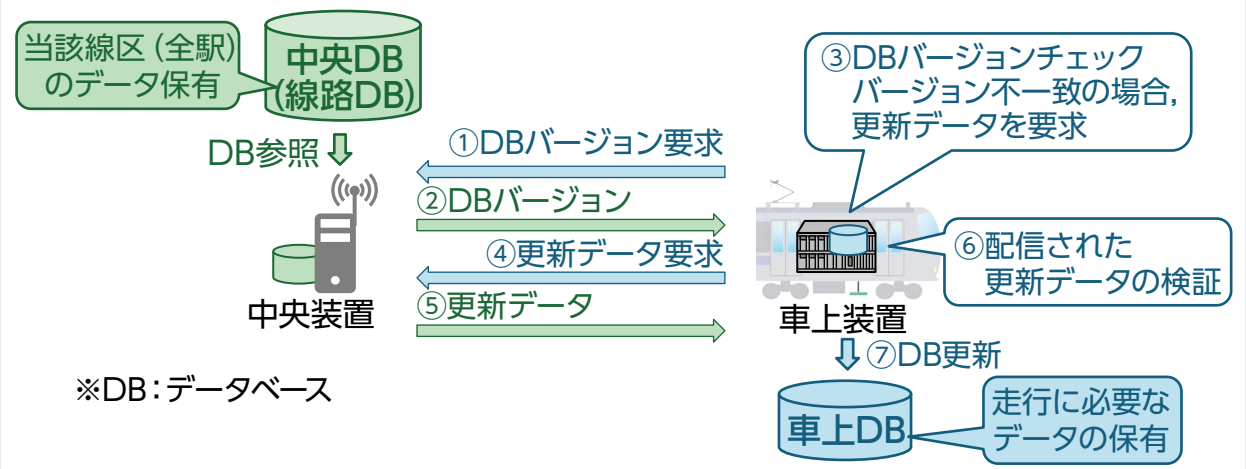

図4　車上データベース更新手順

車上データベース更新手順

作業の省力化と車上データベース更新の柔軟性を実現するため，中央装置にデータを集約して一元管理させる構成としたうえで，車上装置が必要な情報を必要なタイミングで中央装置に要求して配信してもらう方式を採用しました。特に無線式列車制御システムでは，システム構成や運用規模により中央装置に処理負荷が集中することが懸念されています。しかし，この方式は，車上装置が必要なタイミングでデータベース更新処理を実施し，中央装置では要求されたデータを配信する機能のみで実現できるため，中央装置の処理負荷を抑えることができます。

図4に手順を示すように，車上装置が中央装置に対してデータベースのバージョンを問い合わせて，自身の保有するデータベースのバージョンと中央装置からの応答を比較・照合します（①～③）。バージョンが一致する場合は，車上装置が保有している車上データベースが最新であるため更新不要ですが，不一致の場合は，更新が必要です。この場合，車上装置は中央装置に更新データの配信を要求し，配信された更新データを検証して，車上データベースを更新します（④～⑦）。

配信された更新データの検証

公衆通信回線を活用する場合は，なりすましや改ざん，DoS攻撃（Denial of Service attack）☞などの外部の第三者が意図的に誤った制御を誘発するような攻撃への対策が重要です。さらに，車上データベースは運転保安に関わるため，更新データが正当な制御装置から送信されたこと

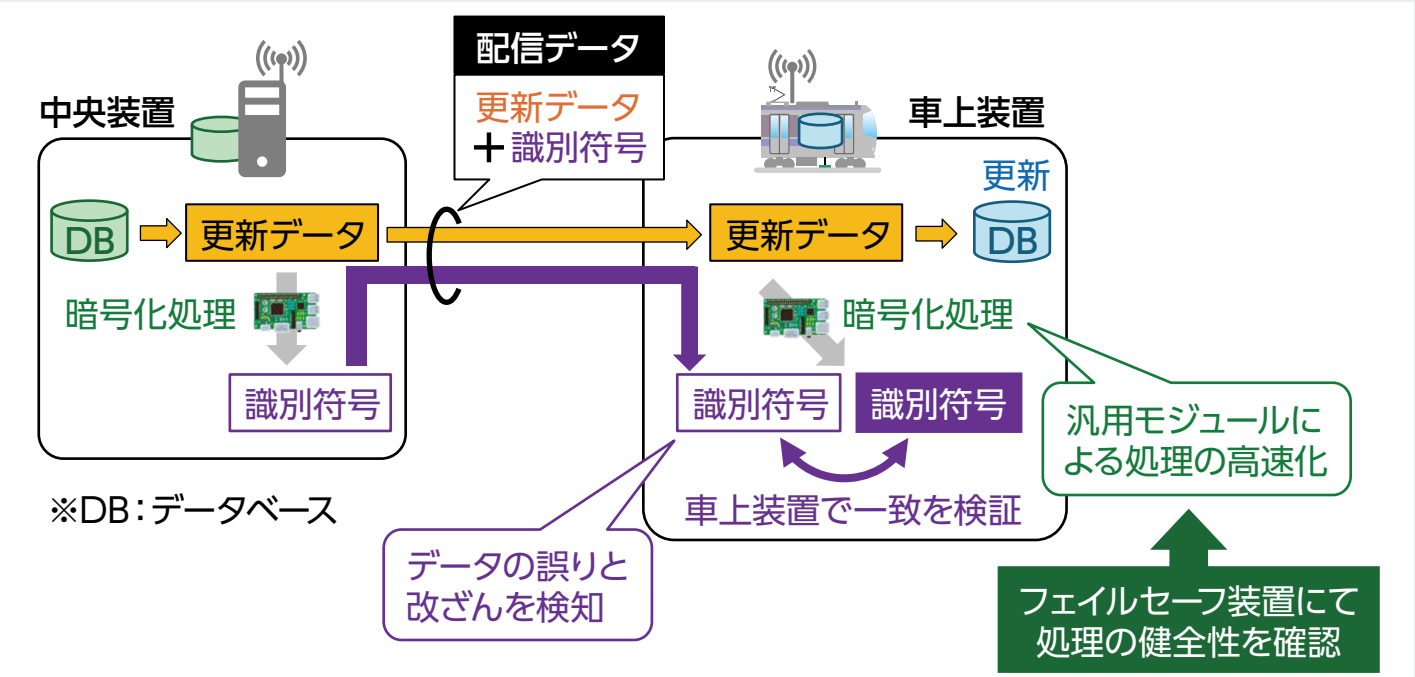

図5　更新データ配信におけるセキュリティー技術

☞ なりすまし，改ざん，DoS攻撃（Denial of Service attack）

なりすましは，外部の第三者がシステム内の装置のひとつであるかのように振る舞い，誤動作を誘発する攻撃です。改ざんは，電文の送受信の過程において第三者が介入して情報を書き換え，誤動作を誘発する攻撃です。DoS攻撃は，攻撃対象の装置に対して無関係な大量の情報を送信することで，正常な動作を阻害する攻撃です。

（真正性）と，送信された更新データがそのままの形で受信できていること（完全性）を検証する必要があります。そこで，汎用で高度なメッセージ認証技術を活用して上記の真正性と完全性を検証する手法を適用しました[1)]。

中央装置は更新データに暗号化処理を用いて生成した識別符号を付加して車上装置に配信します。車上装置では，配信された更新データから識別符号を生成し，更新データと同時に配信された識別符号と比較・照合して一致を確認します。識別符号は更新データに対して唯一性が保証されるため，これらが一致する場合は，更新データに誤りや改ざんなどの改変がないことが確認できます。ただし，識別符号の生成処理については，処理負荷が高いことから非フェイルセーフな汎用モジュールを用いますが，その処理が正常であることについてはフェイルセーフ装置が検証することとします（図5）。

模擬装置による動作確認試験

車上データベース更新手法における各手順の妥当性と識別符号を用いたセキュリティー機能が正常に動作することと，更新データの配信時間を確認するため，模擬装置を試作して動作確認試験を実施しました。動作確認試験では，中央装置と車上装置の模擬装置の間での更新データの配信には，専用に契約したものではない一般の携帯電話利用者と同じ公衆通信回線を使用しました（図6）。車上データベース更新処理の時間については，手順ごとの処理時間について確認し，データ容量の増加に比例して更新時間が増加することを確認しました（図7）。その結果，現在運用されている範囲で想定される容量

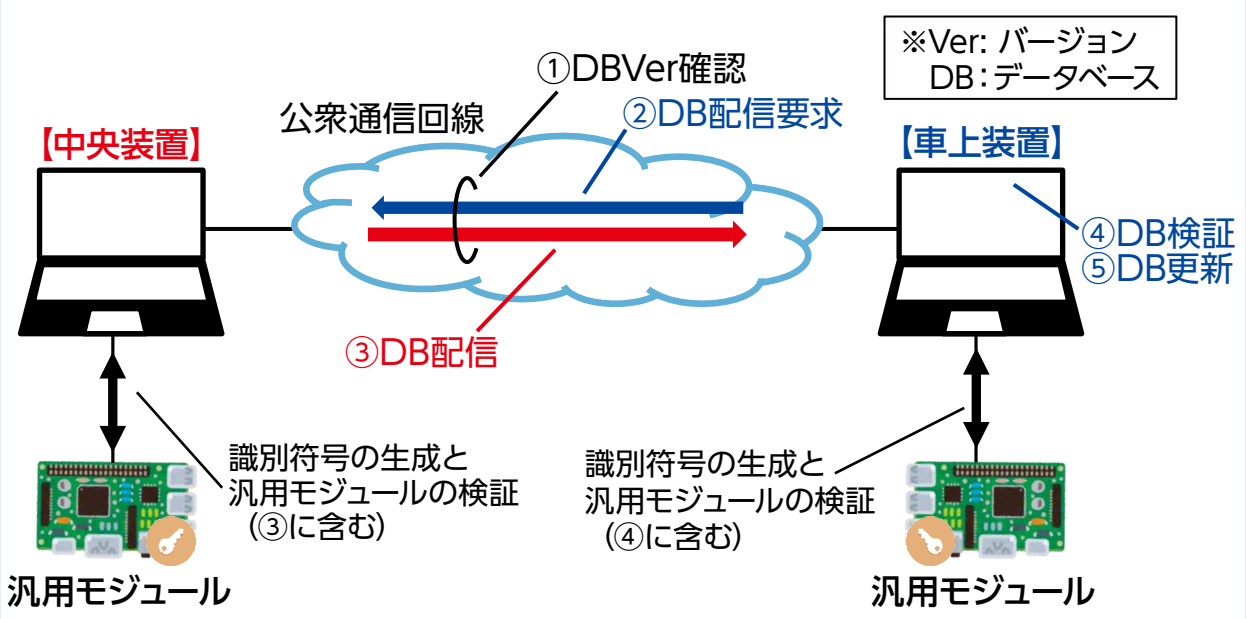

図6　動作検証試験の構成

■配信時間[秒]

データ容量[MB]	①DB Ver確認	②DB配信要求	③DB配信	④DB検証	⑤DB更新	合計
0.5	2	1	1	13	1	18
1.0	3	1	1	24	1	30
2.0	3	1	2	47	1	54
3.0	3	1	2	69	1	76
4.0	3	1	2	91	1	98

※DB：データベース

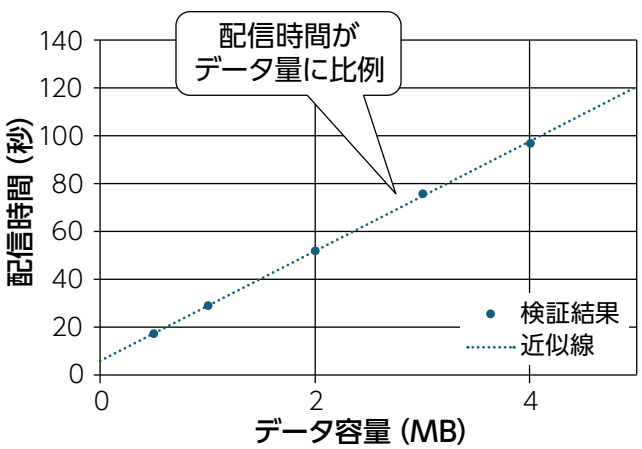

図7　動作検証試験の結果

である4MBでも2分以内に処理が完了することが確認できました。

本技術を応用した新しい運転保安システムの提案

相互直通運転を実施している場合，自社の車両のみならず直通先の他社の車両に対して車上データベースを更新する必要があります。本手法を適用すると，相互直通運転している列車が，次の区間の最新のデータベースを保持していない場合でも，直通区間へ進入する前に自動的にデータを更新して走行を継続することが可能となります。例えば，図8のように，列車が直通先のB区間の最新の車上データベースを有していない場合，進行方向にあるデータベースの境界（A区間→B区間）を認識し，A区間内の駅に停車中に更新データを取得することで，B区間に進入することができます。なお，車上データベース更新時は，あらかじめ次の区間への進入を防護するブレーキパターンを設定したうえで，データベースバージョンが一致する場合もしくはデータベース更新が完了した場合にブレーキ

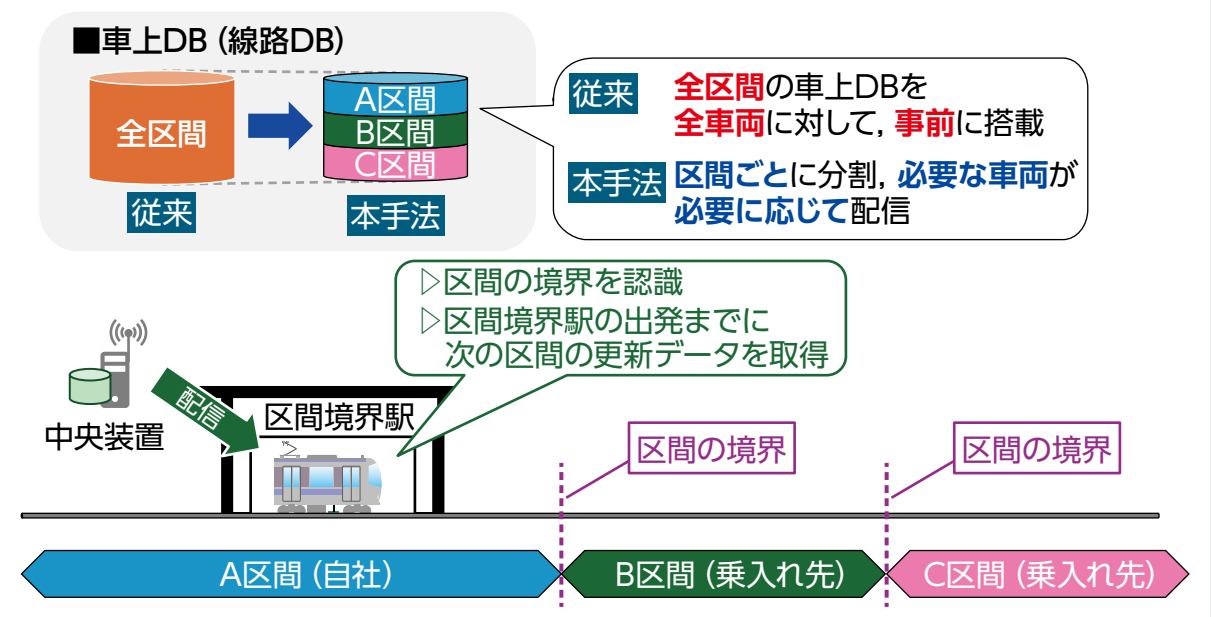

図8　相互直通運転への適用

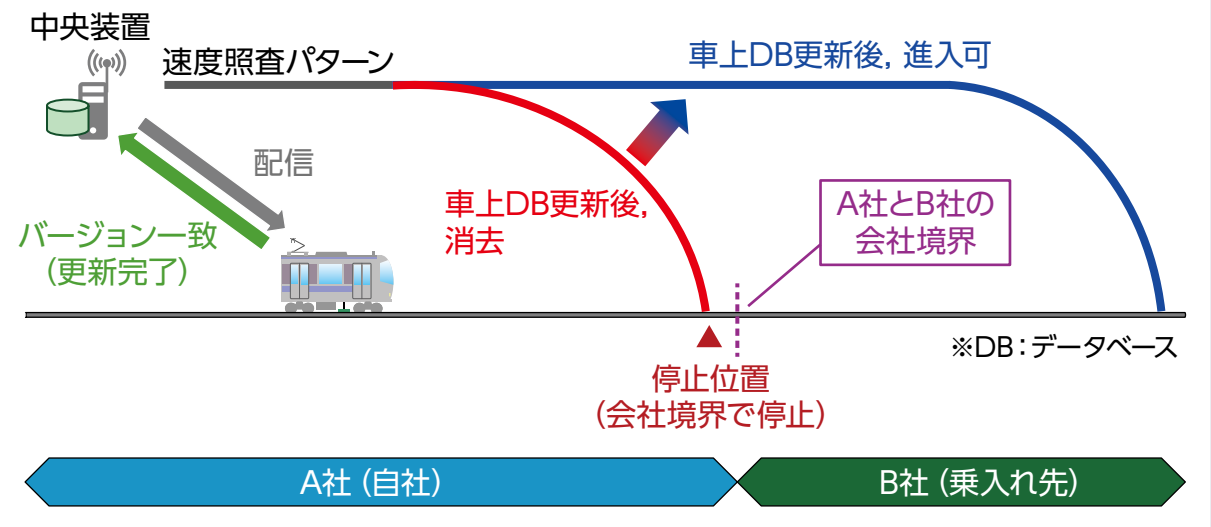

図9　車上データベース更新における列車防護

パターンを消去することで，列車を防護します（図9）。

これにより，相互直通運転において，他社車両への車上データベースの導入に関わる調整や作業に関わる業務が省力化できます。

おわりに

車上データベース更新の省力化と，任意の場所でのデータベース更新の実現に向け，公衆通信回線を活用した車上データベース更新手法を開発しました。開発した手法や機能に対して確認試験を実施したところ，更新場所の制約がなく，かつ係員を介さずに車上データベース更新を実現できる見通しが得られました。

今後は，実システムへの適用に向けて，実際のフェイルセーフ装置を用いた確認試験を実施する予定です。RRR

文　献

1）祇園昭宏，北野隆康，遠山喬，太田佑貴：次世代の鉄道信号をサイバー攻撃から守る，RRR，Vol.81，No.6，pp.10-15，2024