次世代の鉄道信号をサイバー攻撃から守る

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

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

遠山　喬
Takashi Toyama
信号技術研究部
信号システム研究室
副主任研究員

太田　佑貴
Yuki Ota
信号技術研究部
列車制御システム研究室
副主任研究員

はじめに

信号保安システムは，列車の安全・安定輸送を確保するための設備として，図1に示すように，信号保安装置と，鉄道事業者が敷設・管理する伝送路で構成され，沿線に広く設置されています。特に安全を確保するうえでの重要な設備であるため，信号保安装置は故障した際に安全が損なわれることのないように専用の装置として設計されており，信号保安専用の伝送路と組み合わせて使用されています。しかし，専用の装置や伝送路は，導入コストやメンテナンスなどの維持管理コストが大きいという課題があることから，次世代の信号保安システムでは自営の設備を減らすとともに,装置を標準化・共通化していくことが求められます。近年では，シングルボードコンピューター☞などの高機能でありながら，安価である汎用装置や，MVNO☞などから安

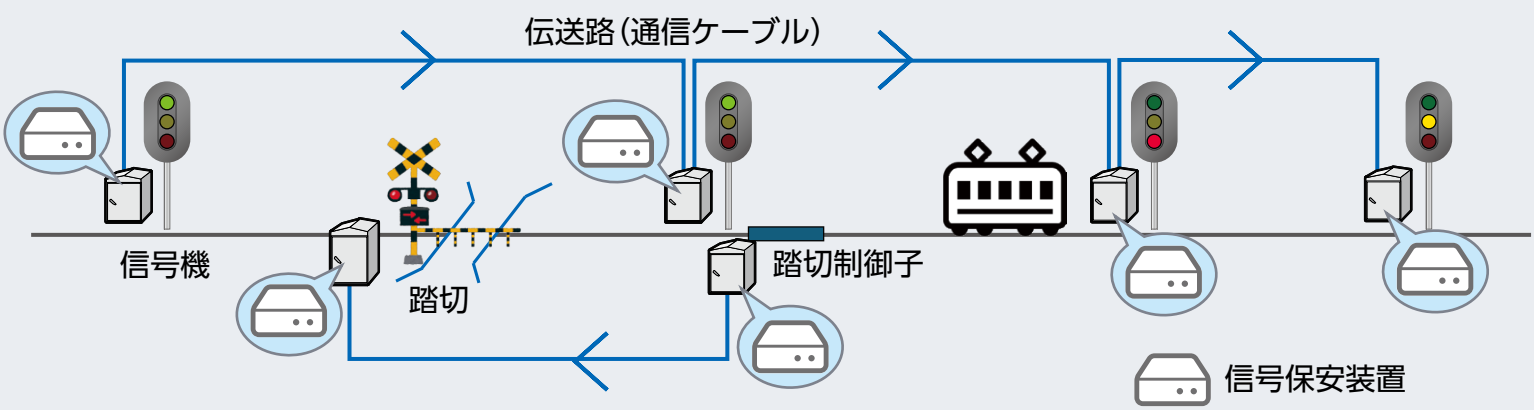
☞ シングルボードコンピューター

Raspberry Piに代表される，一枚の小型プリント基板上にCPUや入出力端子などのコンピューターとしての要素を実装した処理装置。

☞ MVNO：Mobile Virtual Network Operator

仮想移動体通信事業者。移動体通信事業者（MNO）の卸売を受け，通信サービスを提供する事業者。通信速度や通信容量を制限した安価なサービス，IoTなどの特定用途向けのサービスを提供しています。

図1　沿線の信号設備



鉄道沿線の信号保安装置は，装置間で情報の授受を行っていますが
設置間隔が長く，伝送路の敷設と設備の保守にはコストがかかります

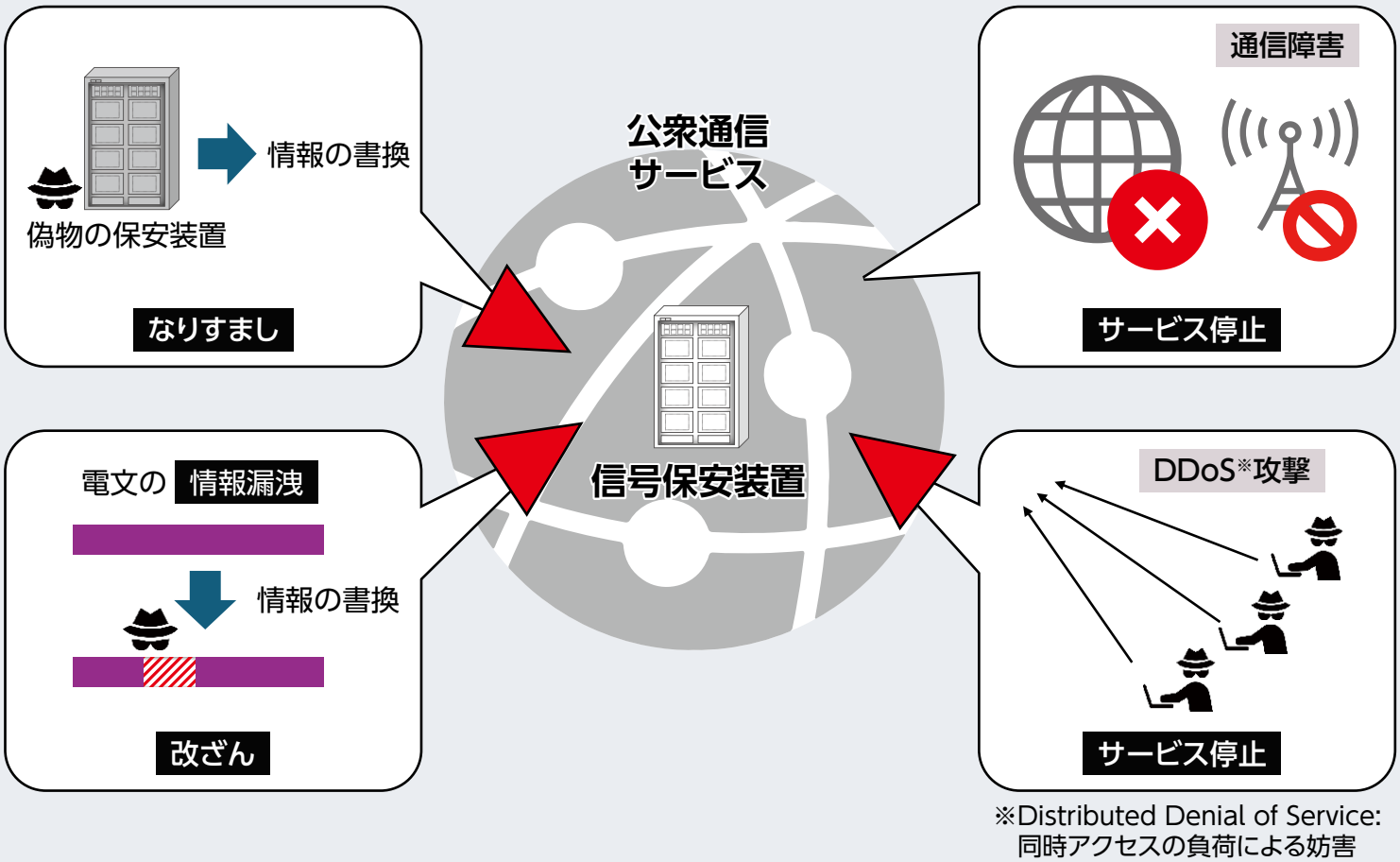


図2　情報セキュリティーの脅威

価な通信サービスなどが提供されており，それらを利用することで，装置や伝送路の低コスト化が考えられます。一方で，公衆通信サービスや汎用装置を利用するうえでは，サイバー攻撃のリスクに対処することが重要となります。

ここでは，鉄道総研が取り組んできた研究から，公衆通信サービス利用・汎用装置利用における課題を挙げたのち，提案したセキュリティー確保手法と，信号保安システムへ適用した構成例を紹介します。

公衆通信サービス利用・汎用装置利用における課題

公衆通信サービスの課題

公衆通信サービスは，鉄道事業者が敷設する自営の伝送路や，通信事業者が提供する専用通信サービスとは異なり，誰でも利用可能な伝送路です。そのため，外部への情報の漏洩と，外部からのサイバー攻撃が想定されます。伝送路におけるサイバー攻撃としては，「なりすまし」「改ざん」「サービス停止」「情報漏洩」などが挙げられます。図2に示すように，信号保安システムの構成装置を偽情報で誤動作させる「なりすまし」「改ざん」が最大の脅威ですが，信号保安システムを通信障害（通信停止や通信遅延）とDDoS攻撃によって稼働できなくする「サービス停止」についても対策が必要です。一般に，信号保安システムで扱う情報は機密性が必要なものではないため，「情報漏洩」そのものはあまり問題になりませんが，攻撃者が入手して手を加えた誤った情報を採用しないよう，「なりすまし」や「改ざん」を識別し排除

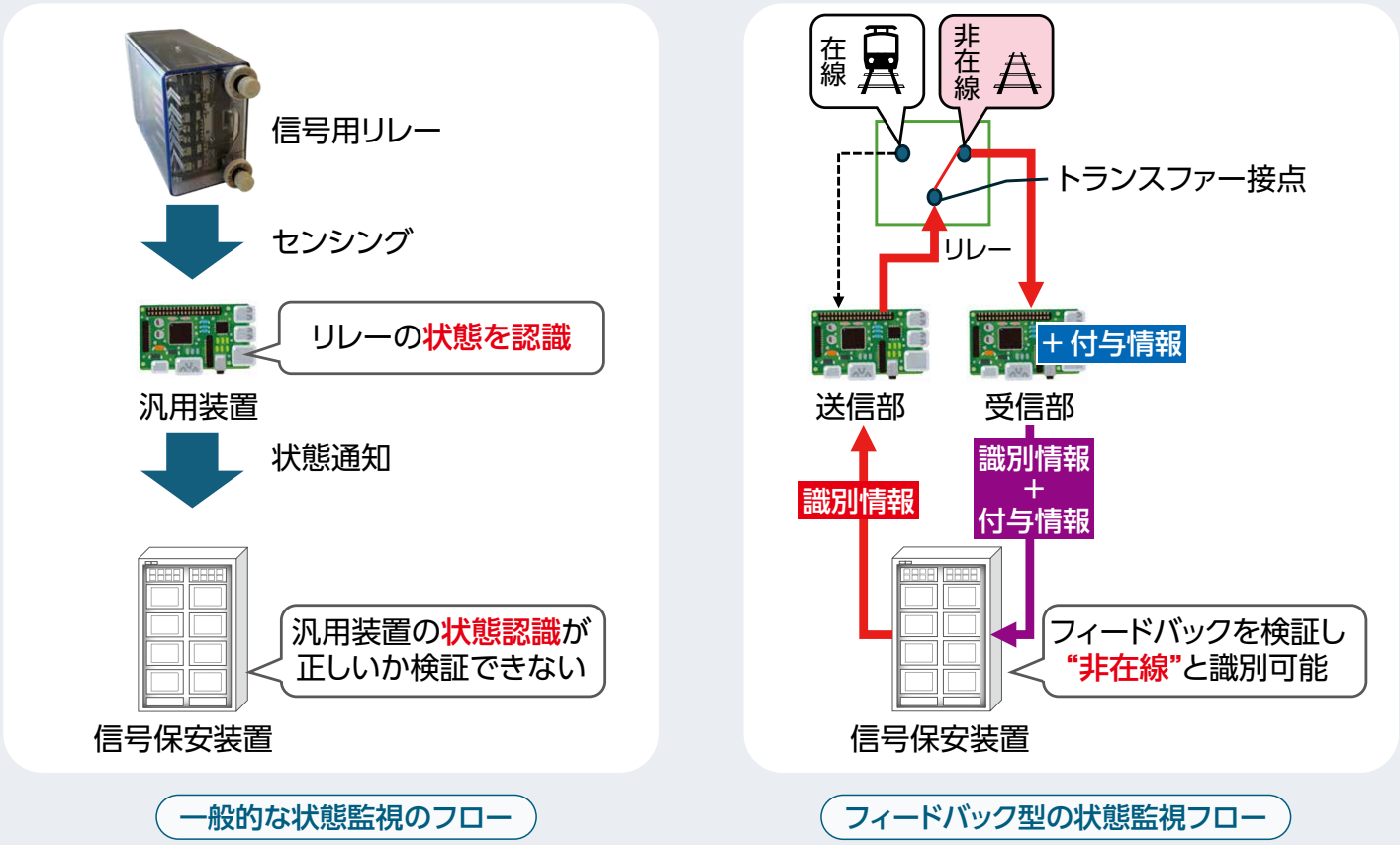


図3　フィードバックループ構成

するなどの対応が必要となります。

また，公衆通信サービス上で安全なデータ通信をするための，VPN☞と呼ばれる接続形態もありますが，VPN機器の脆弱性を狙ったサイバー攻撃が数多く発生しており，脆弱性情報の常時監視と迅速な対策を実施できる体制が求められます。サイバー攻撃に対する対策規模が大きくなるほど，公衆通信サービスの利用によるコスト低減効果が小さくなることが課題です。

汎用装置の課題

信号保安装置は，汎用のCPUやメモリーなどの半導体部品で構成される点は汎用装置と同様ですが，専用設計による故障診断と安全動作を確実に行う機構を備えることでフェイルセーフ性を確保しています。汎用装置は同様の機構を備えていないことから確実な故障診断と，確実な安全動作を保証できません。そのため，汎用装置の利用にあたっては，装置自体の故障を検知し，危険な状態にさせない仕組みを実現する必要があります。

また，情報セキュリティーの観点では，汎用装置自体がサイバー攻撃の踏み台とされて，「なりすまし」「改ざん」「サービス停止」「情報漏洩」に利用されることを想定する必要もあります。

安全性・セキュリティー確保手法の概要

次世代の信号保安システムにおいて汎用装置を利用する際には，フェイルセーフ性の確保と，汎用装置と公衆通信サービスへのサイバー攻撃に対する防護をあわせて実施する必要があります。安全性・セキュリティー確保手法[1)]の実装例として，フィードバックループ構成と，メッ

☞ VPN：Virtual Private Network
仮想専用通信網。暗号化技術により情報伝送の専用の通り道をトンネルのように作って伝送時のデータ窃取や改ざんから保護する通信技術。実現するソフトウェアが公開されており，セキュリティー上の欠陥や弱点を発見・利用されるリスクがあります。

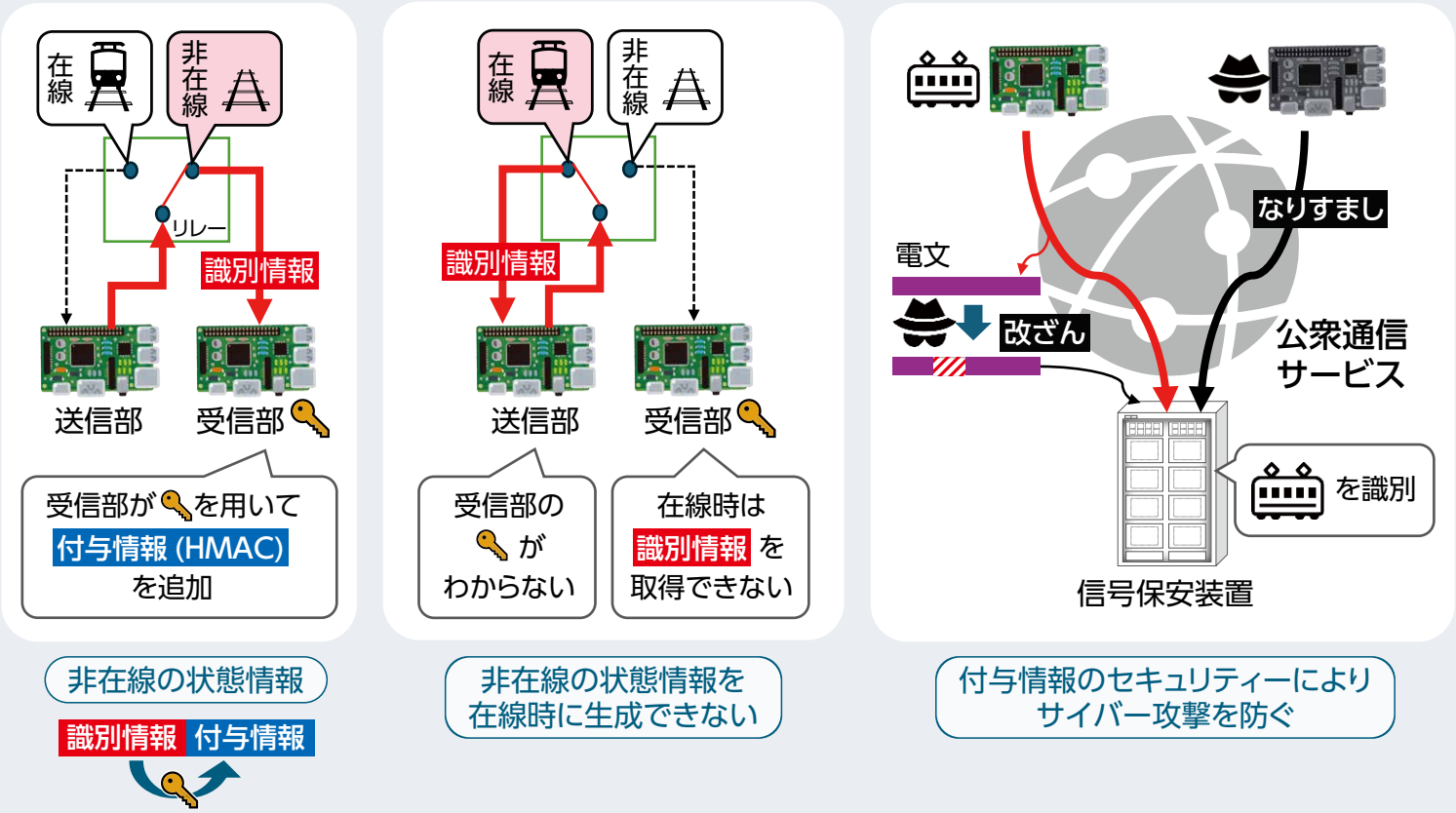


図4　メッセージ認証手法

セージ認証について紹介します。

フィードバックループ構成

列車の在線状態を示すリレーの状態識別を例に，汎用装置を利用する際の安全性確保手法を紹介します。汎用装置がリレーの状態を識別する際に，列車が軌道に在線しているにも関わらず在線を認識しないと，その結果を用いた信号保安装置が後続の列車へ進行現示を出す，踏切の警報を鳴らさずに列車が進来するなどの危険な事象が起きえます。そのため，識別する汎用装置が故障した際にも危険側の誤認がないことが求められます。

汎用装置をリレーの状態識別に用いる場合，汎用装置に接点状態を判断させるのではなく，汎用装置で付与した情報を別の装置で診断する構成とする必要があります。そこで，図3に示すような汎用装置で追加した付与情報を識別情報とあわせて診断する，以下のようなフィードバックループ構成を開発しました。

- 汎用装置は識別情報を送信する送信部と，非在線状態のときに識別情報を取得する受信部の2台を1組として用います。
- 受信部は，リレーのトランスファー接点が非在線に構成されているときにのみ送信部からの識別情報を受け取る回路構成となっています。また，受信部は受け取った識別情報に付与情報を加えて信号保安装置に応答します。
- 信号保安装置は，汎用装置の動作や伝送路が正常で，識別情報に付与された情報が揃っている場合にのみ，列車が非在線となる判定をします。
- 受信部からの応答がない場合や，付与情報が異なる場合は，在線として扱います。

メッセージ認証手法

汎用装置や公衆通信サービスへのサイバー攻撃に対する防護のため，メッセージ認証手法を適用する手法を開発しました。図4に示すよう

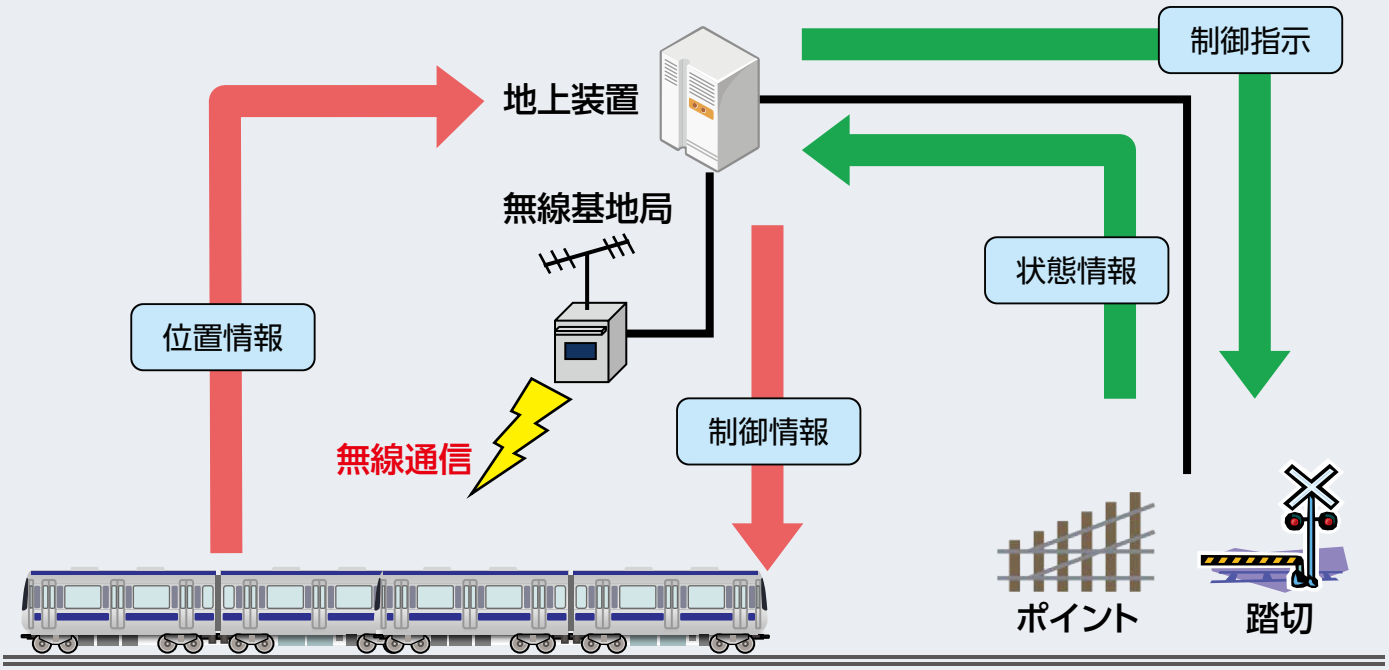


図5　無線式列車制御システム

に，装置IDを鍵情報とするHMAC☞を付与情報とすることで，以下のような仕組みでセキュリティー上の脅威を防ぎます。

- 非在線の状態判定は，受信部の鍵情報により識別情報にメッセージ認証符号が正しく付与される場合となり，応答がない場合や情報が異なる場合は在線状態と判定します。
- 送信部は受信部の鍵情報を知り得ないこと，受信部は在線時に識別情報を取得できないことから，送信部や受信部の故障や不正によって非在線の状態情報を生成することはありません。
- 伝送路上での改ざんやなりすましは，メッセージ認証符号により識別できます。

無線式列車制御システムへの適用

上述のフィードバックループ構成とメッセージ認証手法は，リレーの状態識別の安全性とセキュリティー確保のほかに，無線式列車制御システムでのセキュリティー確保[2)]にも適用することができます。無線式列車制御システムでは，図5に示すように列車と地上装置の間で位置や制御に関する情報を無線でやりとりします。無線設備を公衆通信サービスに置き換えることで沿線設備のさらなる省設備化が可能となりますが，セキュリティー確保が課題となっていました。図6に示すように，地上装置と車上装置に汎用装置によるメッセージ認証符号の生成機構を追加し，列車制御情報（位置情報や制御情報）

☞ HMAC：keyed-Hash Message Authentication Code
メッセージ認証符号のひとつであり，ハッシュ関数と秘密鍵を用いてメッセージのダイジェスト化を行う。SHA 2 - 256を利用する場合，2070年まで使用可能と見込まれます。

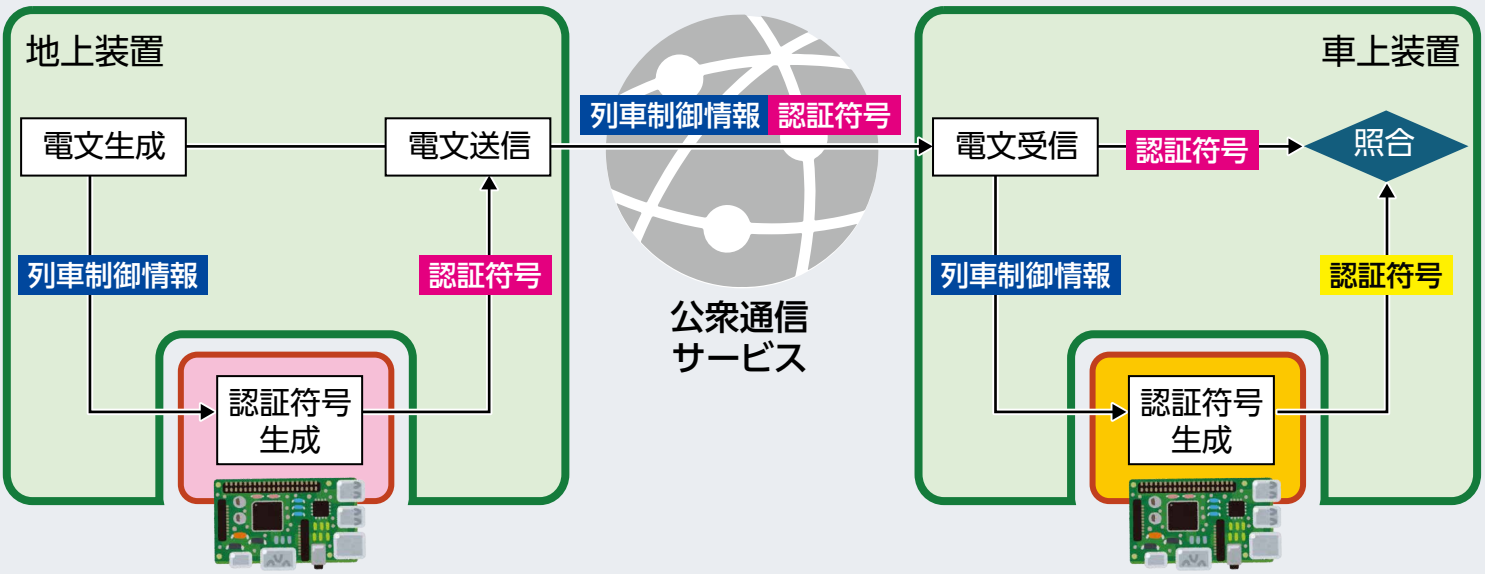


図6　セキュリティー対策の組み込み例

に認証符号を生成・付与して送信する構成とし，受信装置が汎用装置に再生成させた認証符号と受信した認証符号を照合することで，以下のように伝送路のセキュリティーを確保します。

- 伝送路においては，メッセージ認証符号により，改ざん・なりすましから防護します。
- フェイルセーフ装置が汎用装置の故障を診断し，汎用装置の健全性を確保します。
- 汎用装置の更新によりセキュリティーのアップデートが容易に可能です。

おわりに

汎用装置や公衆通信サービスを利用する次世代の信号保安システムで課題となる安全性とセキュリティーの確保について，フィードバックループとメッセージ認証による確保手法と，無線式列車制御システムへの適用について紹介しました。セキュリティーの維持には，対策の継続的な更新を行う必要がありますが，今回紹介した手法は，汎用装置のアップデートにより対応できます。今後，汎用装置と公衆通信サービスを利用した信号保安設備の安全な遠隔監視や，無線式列車制御システムの開発を進めて，省設備化と低コスト化に貢献したいと考えています。

RRR

文　献

1）祇園昭宏，福田光芳，中澤幸弘：汎用端末を用いた保安用途向け接点入出力システムの構成手法，鉄道総研報告，Vol.36，No.8，pp.17-22，2022
2）北野隆康，祇園昭宏：無線式列車制御システムへの汎用通信回線の適用手法，鉄道総研報告，Vol.37，No.3，pp.23-28，2023