特集論文

耐環境型高機能ERPスイッチ

若菜理枝* 中安俊行***
川手竜介** 山形卓矢*
谷口幸子**

Environmentally－resistant and High－functional ERP Switch

Rie Wakana, Ryusuke Kawate, Sachiko Taniguchi, Toshiyuki Nakayasu, Takuya Yamagata

要　旨

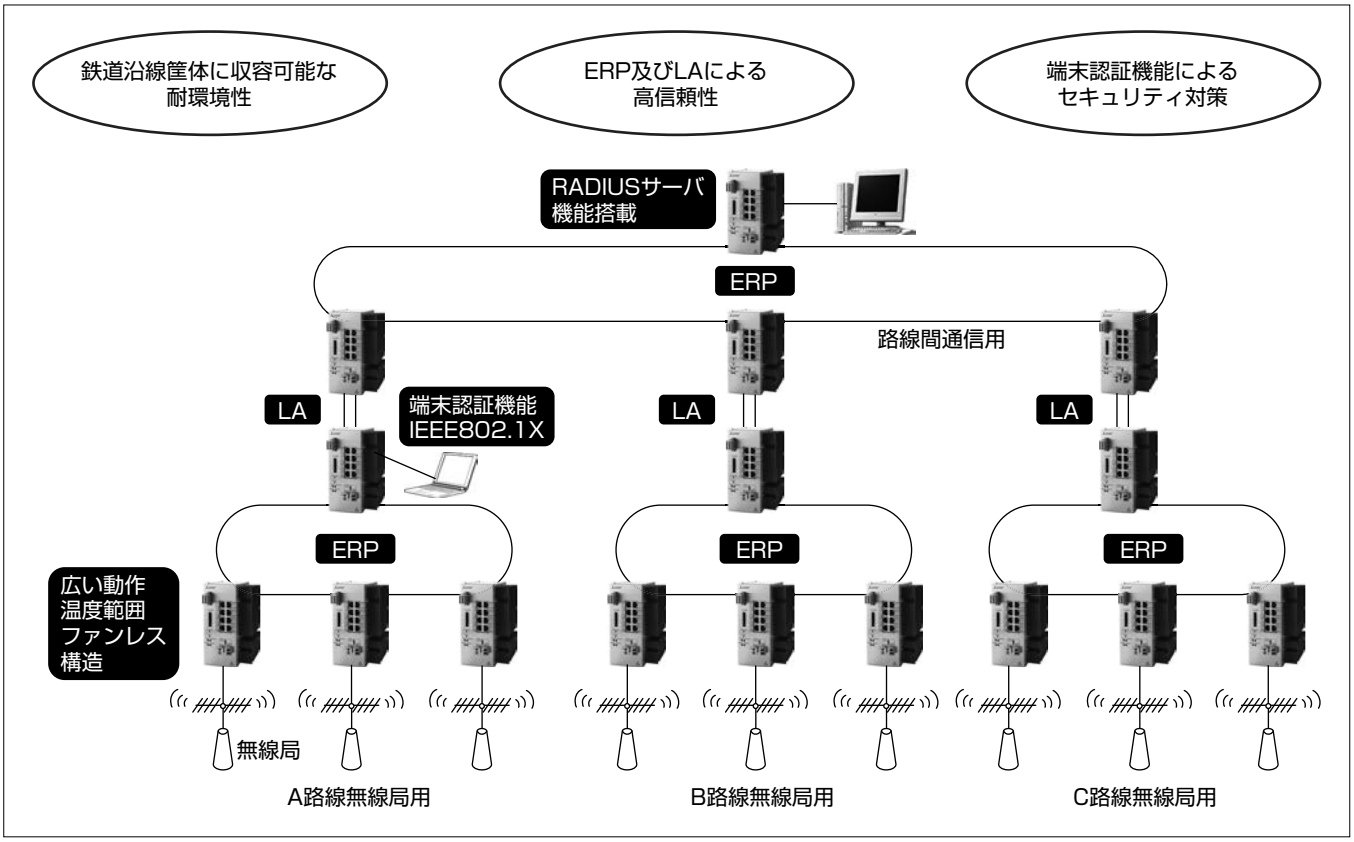
従来の鉄道用ネットワークは，運用分野に合わせ，異なる専用プロトコルを用いて独自のネットワークを構築する場合が多かった。しかし，デジタル通信技術の高度化，Ethernet(注1)の普及に伴い，鉄道用ネットワークでも汎用ネットワークを適用する動きが広がりつつある。

また，鉄道事業者は乗客の大量輸送や高齢化社会への対応の観点から，高密度運転や設備メンテナンスの省力化を実現するシステムの開発・導入に取り組んでいる。

三菱電機は，2016年にEthernet技術を用いた産業用のインテリジェントスイッチを開発しているが，今回は，鉄道信号分野への適用を考慮して，耐環境型高機能ERP(Ethernet Ring Protection)スイッチを開発した。この装置は鉄道沿線筐体(きょうたい)への収容を考慮し，広い動作温度範囲(－20～65℃)に対応する耐環境性を保持している。また，ネットワークに障害が発生した場合でも通信を継続する高信頼性機能(ERP，LA(Link Aggregation))に加え，なりすまし等へのセキュリティ対策となる端末認証機能(IEEE802.1Xに準拠)，RADIUS(Remote Authentication Dial In User Service)サーバ機能を実装している。

この装置の適用先は，運転間隔の最適化と地上設備のスリム化が可能な無線式列車制御システムなど，現場装置を収容するネットワークが挙げられる。今後は，システムの規模に適した装置選定を可能にするラインアップの拡充や保守性を向上させる機能の充実化を図り，この装置の適用範囲を拡大していく。

(注1)　Ethernetは，富士ゼロックス㈱の登録商標である。



耐環境型高機能ERPスイッチの特長と無線式列車制御システムへの適用イメージ

鉄道用ネットワークは耐環境性とネットワークに障害が発生した場合でも通信を継続する高信頼性が求められる。耐環境型高機能ERPスイッチは広い温度範囲で動作し，ファンレス構造である。また，通信障害によるシステムダウンを防ぐERP機能とLA機能の搭載に加え，なりすまし等へのセキュリティ対策となる端末認証機能を実装している。この装置は無線局の収容や監視カメラ，信号設備などの現場装置の収容も可能である。

*通信システムエンジニアリングセンター　**情報技術総合研究所
***コミュニケーション・ネットワーク製作所

1. まえがき

従来の鉄道用ネットワークは，運用分野に合わせ，異なる専用プロトコルを用いて独自のネットワークを構築する場合が多かった。しかし，デジタル通信技術の高度化，Ethernetの普及に伴い，鉄道用ネットワークでも汎用ネットワークを適用する動きが広がりつつある。

当社は，2016年にEthernet技術を用いた産業用のインテリジェントスイッチを開発した。今回，この装置をベースに，鉄道信号分野への適用を考慮した，“耐環境型高機能ERPスイッチ”を開発した。

本稿では，開発したERPスイッチの主な機能と構成技術について述べる。

2. 開発の背景

鉄道事業者は乗客の大量輸送や高齢化社会への対応の観点から，高密度運転や設備メンテナンスの省力化を実現するシステムの開発・導入に取り組んでいる。開発するシステムのネットワークには汎用ネットワーク装置が求められているが，その要件は，広く普及しているオフィスや家庭向け用装置とは様々な差異がある。

今回，鉄道用ネットワークの要件を満たす耐環境型高機能ERPスイッチを開発した。このERPスイッチは，次のような鉄道用ネットワークに適用可能である。

⑴ 列車制御システム用ネットワーク
⑵ 監視カメラ用ネットワーク
⑶ 信号システム用ネットワーク

3. 鉄道用ネットワーク装置の要件

鉄道用ネットワーク装置の要件として，安定輸送を支える高信頼性機能，線路沿線などで使用可能な耐環境性，メンテナンス省力化につながる容易な保守性等がある。

⑴ 高信頼性機能

鉄道用ネットワークは様々な機器が周期的に制御信号を送受信しており，ネットワークに障害が発生した場合でも通信を継続する高信頼性が求められる。また，汎用ネットワーク技術の適用に伴い，なりすまし等のセキュリティ対策機能の実装要求も高まっている。

⑵ 耐環境性

沿線の屋外やトンネル内の筐体に収容可能なコンパクトな形状で，広い温度範囲での動作が必要である。

⑶ 保守機能

装置故障時の迅速な保守対応のため，故障装置の自動検出，故障予知の通知機能，及び保守作業員のスキルによらない装置交換が可能な仕組みが求められる。また，定期的な部品交換を不要とする装置構造も重要である。

4. 主要機能

3章で述べた要件を満たす鉄道用ネットワーク装置として，耐環境型高機能ERPスイッチを開発した。**図1**に装置の外観，**表1**に主要諸元を示す。

図1．耐環境型高機能ERPスイッチ

表1．耐環境型高機能ERPスイッチの主要諸元

項目			内容
通信インタフェース		LANポート	10／100BASE-TX 4ポート 10／100／1000BASE-T 4ポート
		光ポート	1000BASE-X 2ポート
伝送距離		LANケーブル	最大100m
		光ファイバケーブル	5～15km(LXの場合)(注2)
スイッチング速度			最大6.4Gbps
転送方式			カットスルー方式 ストア&フォワード方式
MACアドレス学習数			最大2,048個
VLAN機能			IEEE802.1Q (ポートVLAN・タグVLAN)
高信頼性冗長機能	ERP	ERP設定可能ポート数	2ポート
		ERP切替時間	障害発生から5ms以内 (ERPスイッチ16台接続時)
	LA	LA設定可能グループ数	5グループ
		LA経路切替時間	障害発生から1s以内
	ループ検出	ループ検出対象のVID指定可能数	最大8個
	セキュリティ	MAC SAフィルタリング	最大32エントリ
		端末認証(IEEE802.1x)	認証方式：PEAP-MS-CHAPv2
			RADIUSサーバ機能実装
ハードウェア諸元		動作環境条件	－20～65℃ 5～95%(結露がないこと)
		定格入力電圧	DC24V (許容電圧範囲DC18.0～31.2V)
		外形寸法	97.5(W)×121.0(D)×167.0(H)(mm)
		質量	1.5kg
		冷却方式	自然空冷 (ファンレス・メンテナンスフリー)
		プラットフォーム	FPGAによって実現
保守機能		故障予知の通知	光パワー異常を自動検出
		ログ管理	操作ログ，アラームログ
		遠隔保守	Telnet，SNMP， 遠隔バージョンアップ
		その他	SDカードメモリによる初期設定及びログ保存

(注2) 光ファイバの最大伝送距離は実装する光モジュールによって変更可能

MAC：Media Access Control，SA：Source Address，
VLAN：Virtual LAN，VID：VLAN Identifier，
FPGA：Field-Programmable Gate Array，Telnet：Teletype network，
SNMP：Simple Network Management Protocol

この装置は広い温度範囲(－20～65℃)で動作し，ファンレス構造にした。また，通信障害(通信異常)によるシステムダウンを防ぐリング冗長機能(ERP)とLA機能の搭載に加え，なりすまし等のセキュリティ対策となる端末認証機能を実装している。

主要諸元のうち，この装置の特長であるERP機能と端末認証機能について述べる。

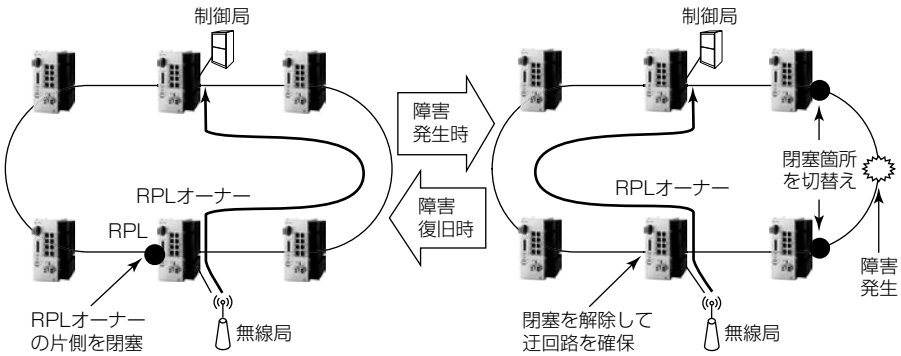


図２．ERPの経路切替え

4.1　ERP機能

ERP機能として，国際規格ITU－T G.8032に準拠したERPを実装している。ERPの経路切替えは，リングを構成するL2SW(Layer 2 SWitch)の１台をRPL(Ring Protection Link)オーナーに設定し，RPLオーナーがリング上の片側(RPL側)ポートを閉塞することでリング内にフレームが循環することを回避する。障害が発生した場合は，障害検出箇所を閉塞すると共にRPLオーナーの閉塞を解除し，リング内の閉塞箇所を切り替えることで通信の継続が可能である(**図２**)。

この装置は当社独自技術である高速切替えモードの実装によって，障害復旧時間を16台接続時５ms以内に短縮している(**表２**)。

4.2　端末認証機能

汎用ネットワーク技術の導入に伴い，なりすまし等のセキュリティ機能の実装要求は高まっている。IEC(国際電気標準会議)では，2002年に鉄道の安全に関わる情報を伝送する通信システムに関する国際規格IEC62280を発行した。この規格にはオープンな伝送システムに対する脅威として，重複，削除，挿入，順序誤り，破壊，遅延，なりすましを挙げている(**表３**)。

鉄道向けネットワークに収容される装置は，無線局や信号装置などの現場端末と，汎用パソコンなどの保守端末がある。現場端末は運用開始後の接続先変更は基本的に発生しないが，保守端末は運用の状況に応じて任意のアクセスポイントに接続する。

この装置は保守端末のなりすましへの対策を強化するため，端末認証機能(IEEE802.1X)を実装した。これによって，悪意のある通信端末からのネットワークアクセスを回避することを可能にした。

4.2.1　IEEE802.1X認証

端末認証では，一般的にIEEE 802.1Xで規定される認証方式が用いられる。IEEE802.1X認証では，認証プロトコルであるEAP(Extensible Authentication Protocol)が使用されるが，EAPには様々なものがあり，使用する認証キー(ユーザーID／パスワード，電子証明書等)や，セキュリティ強度がそれぞれ異なる。そのため，OSのサポート状況や使い勝手等を考慮して，適切なEAPを選択することが必要となる。

保守端末は，一般的にWindows(注4)又はLinux(注5)が搭載されている。EAPの方式を安全性と管理負担を中心に比較検討した結果，セキュリティ強度が高くWindowsパソコンに標準実装され，Linuxでも一般的にサポートされているPEAP－MS－CHAPv2(Protected EAP MicroSoft Challenge Handshake Authentication Protocol version2)を採用した。

端末によるサーバの認証は認証局が発行する証明書を用い，端末の認証はID／パスワードで行われる。情報のやり取りはTLS(Transport Layer Security)トンネル内で行われるので，盗聴の可能性が低く，ID／パスワードを適切に管理することで，安全性が確保できる。

表２．リング冗長方式と経路切替え時間の比較

	切替え時間(注3)(障害復旧時間)	接続条件	規格
今回の装置	５ms以内	16台接続	ITU－T G.8023＋高速切替えモード
	８ms以内	64台接続	
ERP	50ms以内	16台接続	ITU－T G.8023
RPR	50ms以内	50台接続	IEEE802.17
MRP	200ms以内	50台接続	IEC62439

(注３)　今回の装置の切替え時間は実測値，ERP・RPR・MRPは規格値
RPR：Resilient Packet Ring，MRP：Media Redundancy Protocol，ITU－T：International Telecommunication Union Telecommunication standardization section，IEEE：Institute of Electrical and Electronics Engineers，IEC：International Electrotechnical Commission

表３．オープンな伝送システムに対する七つの脅威と定義

脅威	定義
重複	単一のメッセージが２回以上受信される
削除	メッセージがメッセージストリームから除去される
挿入	メッセージストリームにメッセージが追加される
順序誤り	メッセージストリーム中のメッセージの順番が変化する
破壊	メッセージが改変される
遅延	意図した時刻より遅れた時刻にメッセージが受信される
なりすまし	認証されていないメッセージ・ユーザーが認証されているかのように見える

(注４)　Windowsは，Microsoft Corp. の登録商標である。
(注５)　Linuxは，Linus Torvalds氏の登録商標である。

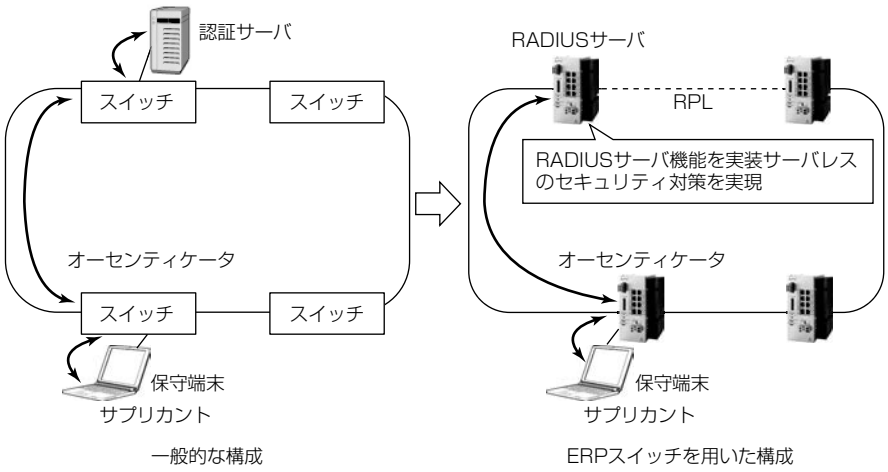


図3．保守端末の接続イメージ

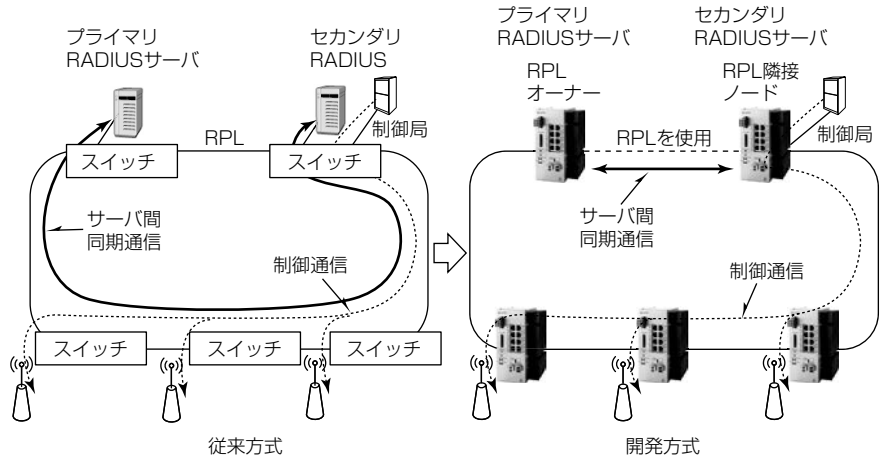


図4．RADIUSサーバ間のデータベースの同期方法

4.2.2　RADIUSサーバ機能の実装

IEEE802.1Xによる端末認証には“サプリカント(Supplicant)”“認証サーバ”“オーセンティケータ(Authenticator)”の三つの構成要素が必要となる。サプリカントは認証を受ける機器(保守端末)であり，認証サーバはサプリカントの認証を行うRADIUSサーバである。オーセンティケータはアクセスポイント(ERPスイッチ)であり，サーバの認証結果を受けてネットワークのアクセス制御を行う。

図3は保守端末の接続イメージである。今回の開発ではオーセンティケータ機能だけでなくRADIUSサーバ機能もERPスイッチに実装することで，サーバレスのセキュリティ対策を可能にした。

保守端末は，あらかじめ認証局から証明書の発行を受けた後，オーセンティケータ機能が有効なERPスイッチに接続する。ERPスイッチはRADIUSサーバと保守端末間の認証結果を受け，保守端末にネットワークへのアクセス制御を行う。

4.2.3　RADIUSサーバの冗長化

ネットワーク上のERPスイッチは２台までRADIUSサーバとして設定でき，冗長構成が可能である。

RADIUSサーバの認証データベースは，悪意ある端末のアクセス履歴などを調べるために有益な情報源となる。RADIUSサーバを冗長化した場合，プライマリRADIUSサーバは認証が完了するとセカンダリRADIUSサーバと認証データベースを同期することにした。また，ERPリングのRPLオーナーとRPLを介して接続するERPスイッチ(RPL隣接ノード)をRADIUSサーバとして設定した場合には，RPLを使用したRADIUSサーバ間の同期通信を可能にした。

このRPLの通信帯域を有効活用する方式によって，冗長サーバ間の同期通信の影響を受けずに，制御通信のリアルタイム性を確保できる(**図4**)。

5. むすび

今回開発した鉄道用耐環境型高機能ERPスイッチは，無線式列車制御システムの地上ネットワークの他，様々なネットワークへの適用が可能である。今後は，システムの規模に適した装置選定を可能にするラインアップを拡充するために，ポート数の少ない製品を開発する予定である。さらに，ネットワークの接続情報，障害情報をERPスイッチ間で転送・集約して保守端末へ通知する，保守性を向上させる機能の充実化を図る開発も計画している。これらの開発によって，この装置の適用分野を拡大していく。

参考文献

(1) 谷口幸子，ほか：ハードウェアベースのリングプロテクション機能評価，電子情報通信学会総合大会，B-8-24 (2013)
(2) 川崎邦弘：安全関連伝送に関する国際規格IEC62280，鉄道総研報告 (2013)
(3) 中安俊行，ほか：CC-Link IEフィールドネットワーク対応インテリジェントHUB，三菱電機技報，**90**，No.6，362～366 (2016)