

セキュア無線システムの運用評価試験

Operation and evaluation test of secure radio system



木村 尚史*



服部 鉄範*



工藤 司**



竹下 剛***



相馬 吉輝**

Radio equipment for railway operation use apply dedicated frequency allocated by Ministry of Internal Affairs and Communications, and severe management is required. It is located as important radio because a serious damage is assumed on the train and maintenance staff when the railway radio is abused when loss or theft occurred. Therefore we developed a “secure radio system” for the purpose of preventing the abuse by a third person after a radio handset has lost or stolen.

In this paper, We report a system outline and a result of operation and evaluation test of the secure radio system.

●キーワード：無線機、セキュリティ、無線機管理、動作許可時間、動作禁止状態

1. はじめに

無線技術の急速な進展に伴い、鉄道分野のさまざまな場面で無線システムが利用されるようになっており、列車無線や業務連絡用としての役割に加え、列車制御におけるデータ伝送といった重要な役割を担うようになってきている。

鉄道で使用する業務用の無線は、総務省から割り当てられた専用の周波数を利用しており、紛失・盗難が発生した際に不正使用されると、列車および保守係員の安全に深刻な影響を及ぼすおそれがあるため、重要無線として位置づけられ厳重な管理が求められている。そのため、無線端末が紛失・盗難された際、第三者による不正使用を防止することを目的とし、セキュア無線端末の開発を行った。

本稿では、この不正使用を防止するために開発を行った無線システムの機能概要および運用評価試験結果について報告する。

2. セキュア無線システム概要

まず、セキュア無線システムの概要について簡潔に説明する。

2.1 セキュア機能概要

本システムは、「動作許可時間」と「動作禁止設定」によるセキュリティ機能を有し、これらの機能によって、無線端末の不正使用を防ぐことが可能となる。

2.1.1 動作許可時間による制御

使用する各無線端末に対して動作許可時間を付与し、動作許可時間のカウントダウンが満了した無線端末は機能がロックされ動作禁止状態となる。動作許可時間の満了によ

て動作禁止状態となった無線端末は動作許可時間が付与されない限り再度使用することはできない。

2.1.2 動作禁止設定による制御

特定の無線端末の使用を停止させたい場合、管理装置から当該無線端末を動作禁止登録し、制御装置から動作禁止信号を受信することで、動作許可時間の満了を待たず強制的に動作禁止状態となる。動作禁止設定された無線端末は、管理装置にて動作禁止を解除したうえで動作許可時間を付与しない限り再度使用することはできない。

2.2 セキュアシステム概要

本システムは、制御装置、無線端末を管理する「管理装置」、無線端末の動作許可時間を制御する「制御装置」、動作許可時間をカウントダウンする「無線端末」で構成される。システムの構成図を図1に示す。

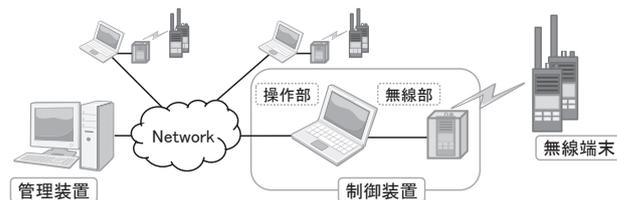


図1 セキュア無線システム構成図

2.3 管理装置

管理装置の機能を以下に示す。

(1) 動作禁止無線端末の管理

すべての動作禁止無線端末情報をリスト化し、接続されている各制御装置へ配信する。

(2) 制御装置の管理

制御装置の盗難防止のため、管理装置との通信が一定時間以上行えない制御装置に対しては動作禁止とする。

2.4 制御装置

制御装置は操作部と無線部から構成されており、周波数が異なる無線端末を3種類まで管理可能である。その場合、それぞれの周波数に対応した無線部が必要となる。

(1) 無線端末への動作許可時間の送信

図2に示すように、制御装置と無線端末間で信号の送受信を行う。制御装置は、当該無線端末が動作禁止無線端末であるかの確認を行い、動作禁止無線端末でなければ動作許可時間を更新し、動作禁止無線端末であれば動作禁止信号を送信し無線端末を動作禁止状態にする。

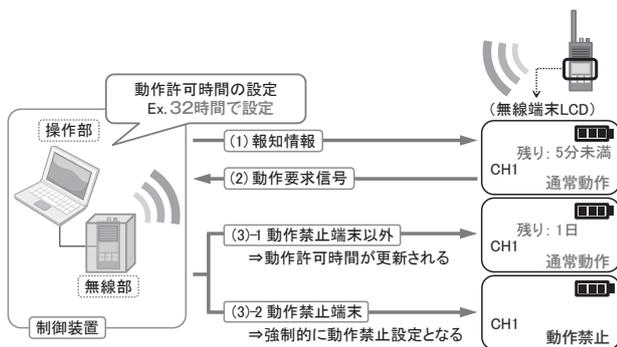


図2 動作許可/動作禁止設定更新フロー

(2) 無線端末動作許可時間の設定

無線端末に与える動作許可時間の指定を行う。

2.5 無線端末

無線端末の機能を以下に示す。

(1) 動作許可時間の更新・カウントダウン

図2で示すように動作禁止端末以外であれば、無線端末の動作許可時間を更新し、動作許可時間のカウントダウンを行う。

(2) 無線端末画面からのセキュア機能状態確認

図3に示すように、無線端末の画面により動作許可時間の残り時間、動作状態の確認が可能である。残り時間については、24時間以上残っている場合は「日」表示、24時間未満の場合は「時間」表示となる。

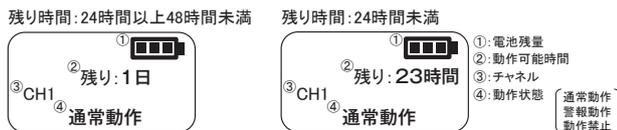


図3 無線端末の画面構成

(3) 電源OFF時の動作許可時間保持

紛失・盗難が発生した際、動作許可時間が減算されないように電源を切った状態で保管し、不正使用する時のみ電源を入れて使用される可能性がある。そのため、ある一定時間経過後には使用できない状態にするため、電源が切られてい

る状態でも動作許可時間のカウントダウンは継続させる。

(4) バッテリー取外し時の動作禁止

紛失・盗難が発生した際、動作許可時間が減算されないようにバッテリーを外した状態で保管し、不正使用する時のみバッテリーを取付けて使用される可能性がある。そのため、バッテリーを外した時点で動作禁止状態にすることで検討した。しかし、通常使用する場合においても現地でバッテリーを取替えることも想定されるため、無線端末に電気二重コンデンサを内蔵し、バッテリーを外した場合でも約5分間は動作状態を継続させる。

3. 運用評価試験概要

運用評価試験は、セキュア無線端末を現場社員に実際に運用してもらい意見を収集する「現地運用試験」と、無線端末台数に対する制御装置の最適なスロット数のシミュレーションを行う「最適スロット数評価試験」に大別される。以下、試験概要および試験結果について説明する。

3.1 現地運用試験

3.1.1 現地運用試験概要

現地運用試験については、事務所で実運用に供せるセキュア機能付の無線端末を設置し、現場社員に実際に10日間使用してもらい、制御装置の画面インターフェイスや無線端末の使用感などのヒアリングを実施し、製品に反映させるべき内容を抽出した。

3.1.2 現地運用試験結果

運用評価試験後のヒアリングの結果、改善要望として以下の3点が抽出された。

- (1) 動作許可時間の更新に1分程度かかり、長いと感じた。30秒位で更新できるとよい。
- (2) 動作許可時間の残り時間の表示は、1日を切ると時間で表示されるが、「1日」、「2日」と表示されている時に残り何時間使えるのかが分かりづらい。
- (3) 動作許可時間の更新時間が3日で設定されている。遠方の現場に行く時は自宅から直行することもあり、場合によっては動作許可時間が3日では足りないことも想定される。

3.2 最適スロット数評価試験

3.2.1 動作許可時間更新の制御シーケンス

動作許可時間更新における制御装置と無線端末間の情報の送受信は、送信タイミングを時分割したスロットにより行

われる。情報の送受信をスロットにより制御することで、情報の衝突を防止する。

制御装置のスロット数4、無線端末4台の場合における制御シーケンスを図4に示す。

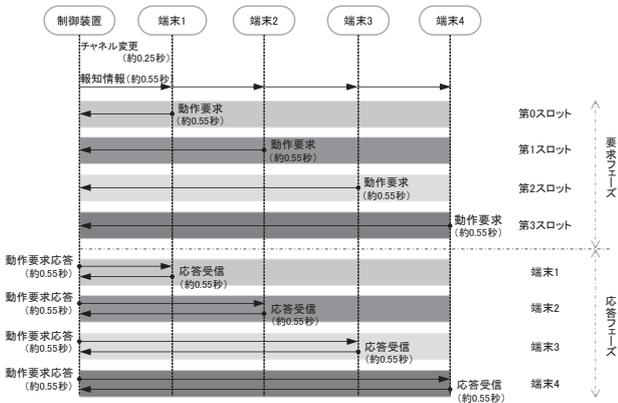


図4 動作許可時間更新制御シーケンス

制御シーケンスは、無線端末が制御装置に対して動作要求を送信する「要求フェーズ」と、制御装置が無線端末に対して動作要求応答を送信する「応答フェーズ」に分けられる。

まず、制御装置は無線部のチャンネルを変更し、各無線端末に「報知情報」を送信する。「報知情報」を受信した無線端末は、制御装置に対して「動作要求」を送信し、動作要求を受信した制御装置は、各無線端末に対して「動作要求応答」を送信する。動作要求応答を受信した各端末は、制御装置に対して「応答受信」を送信し、ここで動作許可時間更新および動作禁止設定が完了する。

また、図4における動作許可時間更新に要する時間は以下に示すとおり、約8秒となる。

要求フェーズ

- ・制御装置のチャンネル変更：約0.25秒
 - ・制御装置の報知情報の送信：約0.55秒
 - ・端末の動作要求の送信：約0.55秒／1スロット
- スロット数=4の処理時間：約3.0秒

応答フェーズ

- ・制御装置の動作要求応答の送信：約0.55秒／台
 - ・端末の応答受信の送信：約0.55秒／台
- 応答端末数4台の処理時間：約4.4秒

図4では、衝突なく情報の送受信が行われているが、端末の台数がスロット数より多くなると、動作要求が衝突してしまうため、スロット割り当てをランダム化することで動作要求の衝突を軽減させた。図5に端末のランダムスロット割り当ての概念を示す。

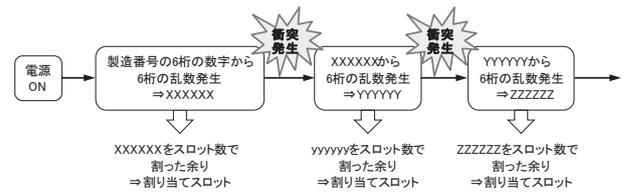


図5 ランダムスロット割り当て

制御装置のスロット数4に対して無線端末の台数が6台の場合において、動作要求が衝突した際の制御シーケンスを図6に示す。

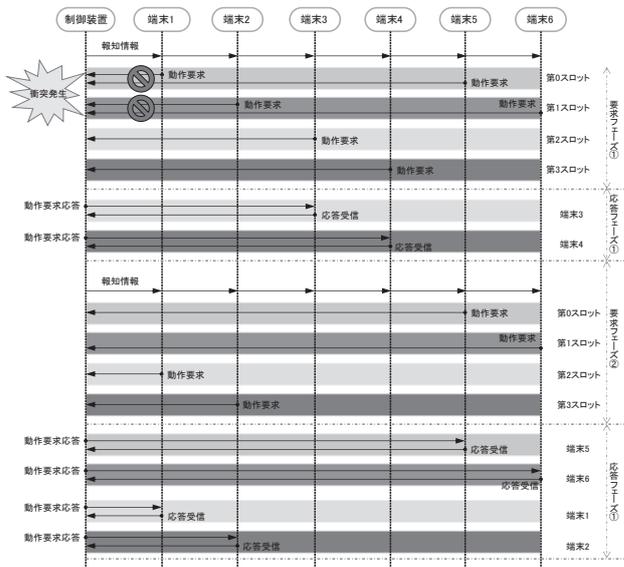


図6 動作要求が衝突した場合の制御シーケンス

- (1) 要求フェーズ①において、端末1、5および端末2、6の動作要求が衝突し、端末3、4は衝突していない。
- (2) 応答フェーズ①において、衝突のあった端末1、2、5、および6は処理されず、衝突のなかった端末3、4は処理が完了する。処理の完了した端末は一定時間報知情報に対して『動作要求』を送信しなくなる。
- (3) 要求フェーズ②において、端末はランダムスロット割り当てを行い、端末が送信するスロットをランダム化する。図6では、残りの端末1、2、5、および6がそれぞれ別のスロットに割り当てられ、衝突が解消されている。
- (4) 応答フェーズ②において、端末1、2、5、および6の処理が完了する。

3.2.2 最適スロット数シミュレーション試験

端末の数に対してスロット数が少なすぎると衝突が頻発し処理ができなくなり、スロット数が多すぎると応答がないスロットが多くなり、必要以上に時間がかかってしまう。そのため、適切なスロット数を以下の手順でシミュレーションにより算出した。

- (1) 報知情報の応答を、1スロットに1台の無線端末だけが応答する確率を求める
- (2) これにスロット数を掛けることにより、このとき処理できる台数の期待値とする
- (3) 期待値を四捨五入し、その回の処理台数とする
- (4) 処理できた台数を、残りの台数から引いた数を、次の回の残り台数とする
- (5) 残り台数が1台になるまで繰り返す

表1にスロット数4、端末数10台の場合の処理回数の計算例を示す。

表1 処理回数の計算例

残り端末数	処理済端末数	1スロットに1台だけ応答する確率	処理できる期待値	処理端末
10台	0台	$(3/4)^9 \times (1/4) \times 10 = 18.8\%$	$18.8\% \times 4 = 0.75$	1台
9台	1台	$(3/4)^8 \times (1/4) \times 9 = 22.5\%$	$22.5\% \times 4 = 0.90$	1台
⋮				
3台	7台	$(3/4)^2 \times (1/4) \times 3 = 42.2\%$	$42.2\% \times 4 = 1.69$	2台
1台	9台	$(3/4)^0 \times (1/4) \times 1 = 25.0\%$	$25.0\% \times 4 = 1.00$	1台

処理時間=(要求フェーズ時間×処理回数)+(応答フェーズ時間×全処理台数)
 =(3.0秒×8回)+(1.1秒×10台)
 =35秒

前記シミュレーションを、端末台数が1~30台の場合に対して、スロット数=4, 8, 16, 32および64をパラメータとして実施した結果を表2に示す。

表2 スロット数別処理回数と処理時間

端末数 [台]	スロット数=4		スロット数=8		スロット数=16		スロット数=32		スロット数=64	
	回数	処理時間	回数	処理時間	回数	処理時間	回数	処理時間	回数	処理時間
1	1	4.1	1	6.3	1	10.7	1	19.5	1	37.1
5	3	14.5	2	15.9	2	24.7	2	42.3	1	41.5
8	6	26.8	3	24.2	2	28	2	45.6	2	80.8
10	8	35	4	31.8	3	39.8	2	47.8	2	83
15	-	処理不可	6	47.7	4	54.9	3	71.7	2	88.5
20	-	処理不可	9	68.8	4	60.4	3	77.2	2	94
25	-	処理不可	14	100.3	5	75.5	3	82.7	3	135.5
30	-	処理不可	19	131.8	6	90.6	4	106.6	3	141

端末台数が8台の場合の最適スロット数は、処理時間が24.2秒と最も短いスロット数8ということになる。また、表中の処理不可は、衝突を繰り返して処理できないことを表している。

シミュレーションの妥当性を確認するため、8台の端末を使用して処理時間の測定を行い、表2に示した端末数が8台の場合の各スロットにおける処理時間と、実測した処理時間を比較した。測定構成図を図7に示す。

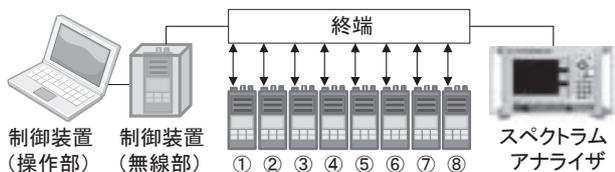


図7 処理時間測定構成図

3.2.3 最適スロット数シミュレーション結果

8台の端末における処理時間について、シミュレーションによる値と実測値の比較を行った結果、表3に示すとおりシミュレーションと実測値はほぼ一致しており、シミュレーションの妥当性が確認できた。

表3 スロット数別処理時間比較表(端末8台)

	スロット数=4	スロット数=8	スロット数=16	スロット数=32	スロット数=64
シミュレーション	26.8秒	24.2秒	28秒	45.6秒	80.8秒
実測結果	27.1秒	24.3秒	30秒	49.3秒	84.8秒

※実測は、10回の平均値

3.3 運用評価試験のまとめ

現地運用評価試験で抽出された3点の課題について、以下のとおり対応した。

- (1) 動作許可時間の更新時間が長い
 報知情報送信周期の変更により更新時間を短縮する
- (2) 動作許可時間の残り時間の表示が分かりづらい
 動作許可時間が96時間以上残っている場合に「日」表示とした。(図8)

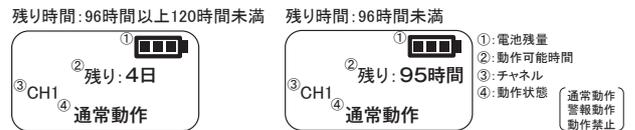


図8 動作許可時間表示の変更

- (3) 各職場の制御装置で動作許可時間を設定
 各職場の制御装置で設定させることは可能である。しかし、すでに導入されているセキュア無線の設定値を3日で統一しているため、運用整理が必要となる。

4. おわりに

無線端末が紛失、盗難された際の第三者による不正使用を防止することを目的としてセキュア無線システムの開発を行った。また、運用評価試験では操作性の改善および本システムを使用する際の最適なスロット設定値として、無線端末数ごとの最適なパラメータを示すことができた。一部の無線端末では本システムを導入し使用を開始しており、今後、ほかの無線端末にも導入していく予定である。