セキュア無線システムの開発


大森　裕明*

鈴木　祐輔**

中井　義*

栗田　明*

立石　幸也*

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、厳重な管理が求められている。鉄道無線は紛失・盗難の際に悪用されると、列車運行に深刻な影響を及ぼすおそれがあるため、警察無線や消防無線と同様に、総務省により重要無線として位置づけられている。そのため無線端末が紛失、盗難された際には、第三者による不正な使用を防止することが重要となる。本開発では、この不正使用を防止することを目的としたシステムに関する検討を行い、紛失・盗難に対応できるセキュア無線システムを開発し、試作品を用いてフィールド試験を実施した。

●キーワード：無線機、無線管理、セキュア

1. はじめに

近年の無線技術の発展により、無線技術を導入した列車制御や、列車無線でデータ伝送を行うといったように、鉄道分野においても無線システムが大きな役割を果たすようになってきた。

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、厳重な管理が求められている。鉄道無線は紛失･盗難が発生した際に悪用されると、列車運行に深刻な影響を及ぼすおそれがあるため、警察無線や消防無線と同様に総務省により重要無線として位置づけられている。

そのため無線端末が紛失、盗難された際には、第三者による不正な使用を防止することが重要となる。

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検討内容、機能概要、動作試験結果について報告を行う。

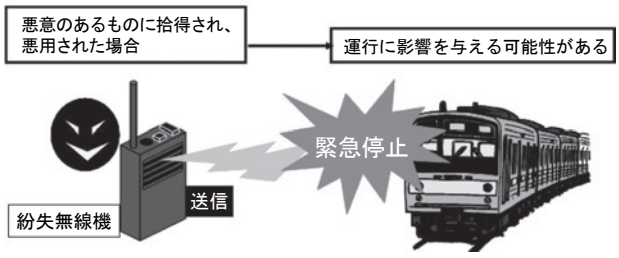

図1　鉄道における無線端末の不正使用例

2. 鉄道における無線端末の主な使用法について

2.1　基地局・陸上移動局間の無線通信

基地局・陸上移動局間で鉄道における無線システムとして多く使用されている形態としては、図2に示す指令と列車との間で用いられている列車無線などが該当する。

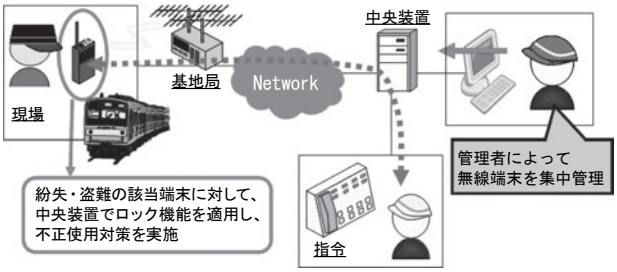

図2　列車無線における不正使用防止概念図

基地局から中央装置を経由して通信を行う場合、無線端末から送信される無線端末の個別番号を中央装置で監視することができる。そのため紛失・盗難などに遭った無線端末の個別番号を登録すれば、中央装置から基地局を通じて無線端末の機能をロックさせ、不正使用ができないよう対策を行うシステム構成とすることが可能である。

2.2　陸上移動局・陸上移動局間の無線通信

陸上移動局・陸上移動局間で鉄道における無線システムとして多く使用されている形態としては、図3に示す列車見張員と作業員との間で使用する作業用無線などが該当する。

*JR東日本研究開発センター　先端鉄道システム開発センター
**高崎支社　設備部　信号通信課（元　先端鉄道システム開発センター）

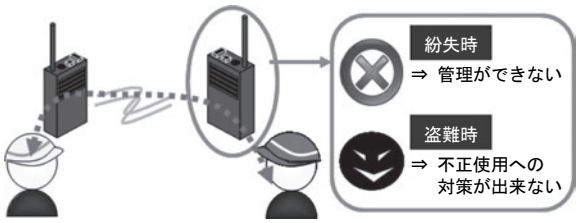

図3　作業用無線使用時における課題

このシステムに類する陸上移動局については、無線端末同士で通信を行うため、通話の相手側が不正使用されている無線端末かどうかの判断を行うことができない。

そこで本開発では、陸上移動局・陸上移動局で通信を行う無線端末について、紛失・盗難などが発生した際に不正な使用を防ぐことを目的としたシステム（以下、セキュア無線システムと省略）の開発を行った。

3. セキュア無線の開発にあたって

3.1　セキュリティ確保の方法の検討

無線端末が盗難にあった際の、セキュリティの確保に対する方法について検討を行った。

案1　使用許可パスワード（固定）の付加された無線端末

固定のパスワードを入力することで無線端末を使用できる仕様とする。しかしパスワードが一度外部に漏れてしまった場合、永続的に無線端末を使用できてしまう。

案2　使用許可パスワード（変動）の付加された無線端末

一定期間ごとに変動するパスワードを入力することで無線端末を使用できる仕様とする。しかし変動するパスワードを決定する装置と併せて盗難された場合、永続的に無線端末を使用できてしまう。

案3　GPSによる動作可能エリアの制限

使用エリアの制限にGPSを用いて、指定したエリアのみ使用できる仕様とする。しかし当該エリア内であれば盗難された無線端末でも使用できてしまう。またGPSが使用できないトンネル内などでの実運用が制限される。

上記検討案から、セキュア無線システムには以下の3点の機能が必要となることがわかった。

①永続的な使用許可を避ける。
②同箇所の装置すべての盗難でも停止できる。
③使用場所に関わらず動作を停止できる。

3.2　動作許可時間による制御

3.1項①の対策として、使用する各無線端末に対して動作許可時間を付与し、その時間が切れると再度動作許可時間を付与しなければ使用できない、という時間制限付のシステムとすることにした。

この機能を用いることで、動作許可時間という基本的な機能での制限が可能となり、管理者側は使用前に想定の時間を付与することで、それ以上の時間における無線端末の使用を禁止できる。

また動作許可時間の機能を用いることで、3.1項③の対策も併せて行うことができる。

3.3　動作許可時間付与装置の上位装置の設置

動作許可時間による制御を行う場合、無線端末に動作許可時間を付与する装置については、基本的に無線端末と同箇所に配置されるため、無線端末と併せて盗難にあう可能性が高い。しかし別箇所に配置すると、無線機を使用する都度、動作許可時間を付与するために別箇所に移動する必要があり、多大な労力を要する。

そこで3.1項②の対策としては、動作許可時間を付与する装置の上位に別の装置を設置することとし、常にネットワーク上で監視を行うこととした。そのネットワーク上から外れた場合、動作許可時間付与装置自体が使用できない仕様とすることで、同じ箇所に設置されている装置すべてが盗難されても不正な使用が防止できる。

4. システム動作概要

4.1　システム概要

本システムは図4に示すように

・動作許可時間をカウントダウンする「無線端末」
・無線端末の使用許可時間を制御する「制御装置」
・制御装置、無線端末を管理する「管理装置」

から構成される。

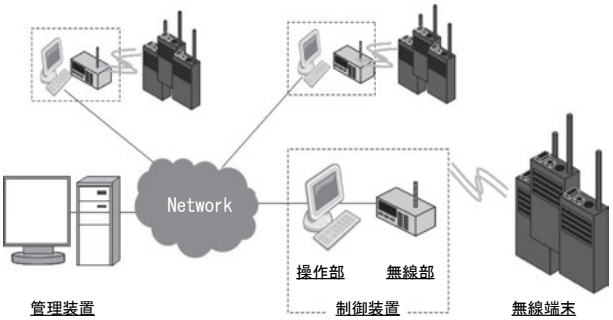

図4　セキュア無線システム構成概要図

図5に示すように無線端末の紛失、盗難の場合には、まず動作許可時間のカウントダウンにより動作許可時間の満了した無線端末は機能が自動的にロックされる。そして管理装置で動作禁止に設定された無線端末は、制御装置による使用許可時間の延長ができず、無線端末の不正使用を防ぐことができる。

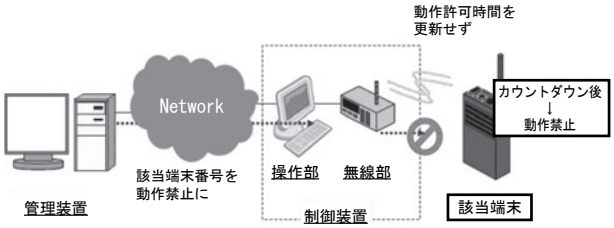

図5　セキュア無線システム動作概要図

4.2　管理装置

管理装置の機能について図6に示す。

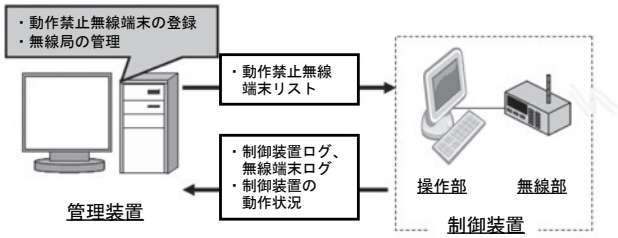

図6　管理装置の機能

(1) 動作禁止無線端末の管理

管理装置に動作禁止無線端末の情報を追加することで、すべての動作禁止無線端末情報をリスト化し管理を行う。そのリストについては、接続されている各制御装置へ配信を行うこととした。

(2) 制御装置の管理

各制御装置に識別番号を設定し、それらを管理装置側で制御装置ID、使用場所、動作履歴を登録・管理する。制御装置の盗難防止のため、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。

(3) 制御装置、無線端末のログ収集

一定時間ごとに制御装置と通信を行い、管理装置から制御装置が受信した内容のログや、制御装置から無線端末への送信した内容のログの収集を行う。

4.3　制御装置

制御装置の機能について図7に示す。制御装置は操作部と無線部から構成されている。また、使用する周波数が異なる複数の無線端末を対象にする場合、制御装置の無線部もそれぞれの周波数に対応する必要がある。

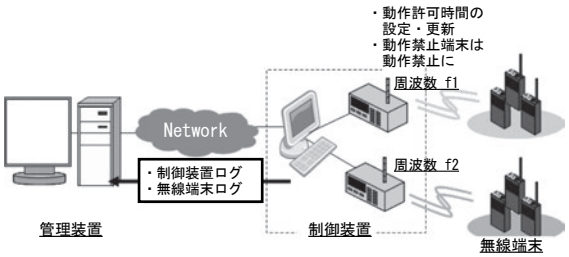

図7　制御装置の機能

(1) 無線端末への動作許可時間の送信

図8に示すように、まず制御装置のメイン画面で報知信号を送信する。その報知信号を受信した無線端末からの動作要求信号を受信すると、当該無線端末が動作禁止無線端末であるかの確認を行う。そして動作禁止無線端末であれば動作禁止信号を送信し、動作禁止無線端末で無ければ動作許可時間の更新を行う。

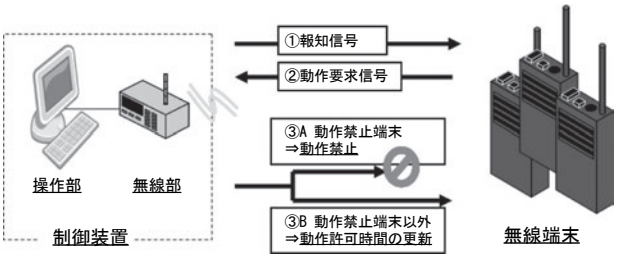

図8　制御装置と無線端末との送受信内容

(2) 無線端末動作許可時間の設定

動作許可時間については、制御装置の設定画面にて時間の指定を行う。

(3) 管理装置への報告用制御情報の蓄積

管理装置で確認できる制御装置ログ、無線端末ログを作成する。

4.4　無線端末

無線端末の機能について図9に示す。

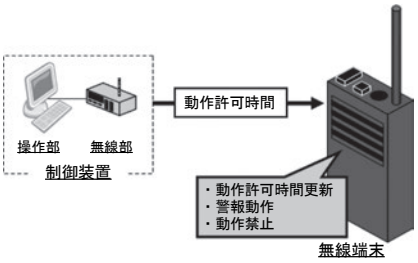

図9　無線端末の機能

(1) 動作許可時間の更新

図9で示すように動作禁止端末以外であれば、制御装置から動作許可時間更新の信号を受信することで、無線端末の動作許可時間を更新する。

(2) 無線端末画面からのセキュア機能状態確認

無線端末の画面により、図10に示すように現在のセキュア機能状態が確認できるようにした。

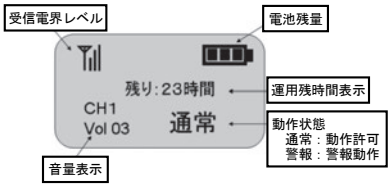

図10　無線端末の画面構成

(3) 動作許可時間後の警報動作

動作許可状態から動作禁止状態までの間に、警報動作状態を存在させた。警報動作とは、動作禁止状態となるため当該無線端末が使用できなくなることを、音で注意喚起を行うものである。具体的には、通話の相手方にビープ音を発生させることとした。このビープ音は、動作しても通話に支障が無いように音量を考慮した。

図11に示すように、警報動作状態となった無線端末については、

・使用者は、無線端末の画面により確認

・通話の相手方は、通話中のビープ音により確認

することにより、通話中で気付かない間に動作禁止状態となることがないよう、二重に防ぐこととした。

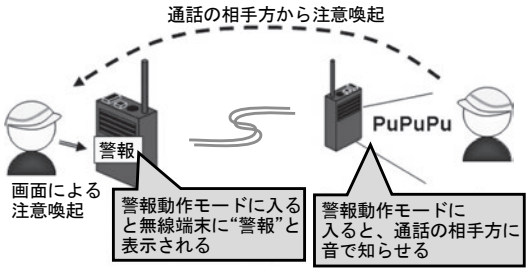

図11　警報動作での動作許可時間終了の注意喚起

(4) 警報動作時間が終了した無線端末の動作禁止

動作許可時間が終了し、その後の警報動作時間も終了した無線端末については、動作禁止となる。動作禁止状態となった無線端末については、制御装置から動作許可信号を受信しない限り、動作許可状態にはならない。

(5) 電源OFF時の動作許可時間保持

通常、無線端末を現場へ持ち運ぶ際には、電源が切られている。そのため、電源が切られている状態でも動作許可時間は保持できるようにした。

(6) バッテリー取外し時の動作禁止

バッテリーを取外した際は、再度取付けたとしても、無線端末は動作禁止状態とした。動作許可状態となるためには、制御装置からの動作許可信号を受信することが必要である。

4.5　動作許可時間更新における制御フロー

無線端末の動作許可時間更新について、制御装置と無線端末間の処理を、無線端末3台を例に図12に示す。

制御装置は報知情報を出す前に無線部のチャンネル変更し、「報知情報」を送信する。

制御装置からの「報知情報」を無線端末が受信すると、各無線端末は「動作要求応答」を制御装置に対して送信する。

動作要求を送信するタイミングを時分割することにより輻輳を制御する。時分割したそれぞれのタイミングをスロットと呼ぶ。無線端末は、ID別に指定された固定スロットで応答する。

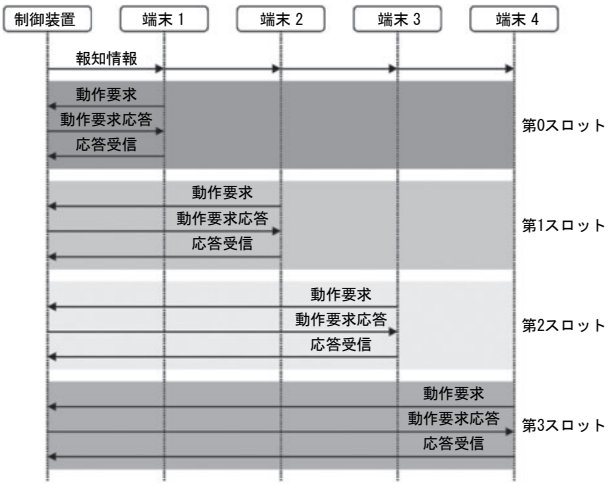

図12　無線端末動作許可時間更新フロー

5. 試験結果

5.1　JR-IPNet上での試験

製作した試作品を用いて、工場内試験だけでなく、将来的な実導入を想定し、JR-IPNet（当社の社内ネットワークの呼称）で試験を行うこととした。

当社内での一般的な無線端末管理方法を考慮した際に、

管理装置：本社、支社

制御装置：現業機関（駅、車両センターなど）

無線端末：制御装置と同箇所

となるため、今回の試験においては以下の2構成にて動作試験を実施することとした。

(a) 管理装置：八王子支社

制御装置、無線端末：八王子信号通信技術センター

(b) 管理装置：本社

制御装置、無線端末：八王子信号通信技術センター

また当社内での将来的な運用形態を考慮した際に、管理装置および制御装置の操作部については、専用サーバー、もしくは、各所管理者の業務用端末に導入することが考えられる。専用サーバーでは考慮する必要が無いが、業務用端末については日常使用している社内業務アプリケーションとの競合を試験する必要がある。そのため管理装置および制御装置の操作部について、業務用端末を用いて試験を行った。

上記の構成で試験を行った結果、他の社内業務アプリケーションとの競合は発生せず、動作許可時間の更新、該当端末への動作禁止制御、警報動作機能、ログ収集などが確実に行われることを確認することができた。

また動作許可時間の更新試験において、無線端末を3台、スロット数を4にして実施した、動作許可時間に関する処理

時間を図13に示す。1スロットにつき1.3秒必要とし、全体の処理を終えるのに約6秒必要となる。

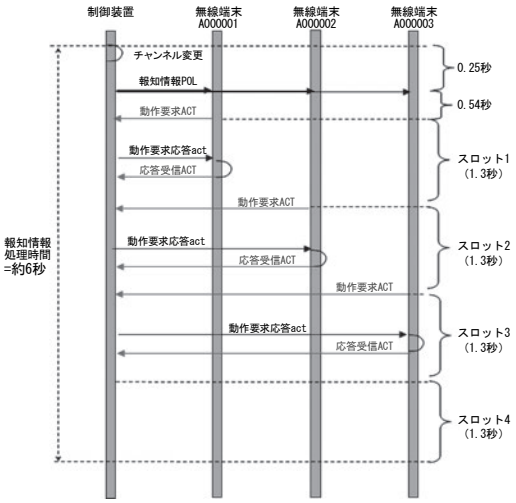

図13　動作許可時間更新に関する処理時間

5.2　無線環境試験

試作無線機におけるBER（ビット誤り率）、RSSI（受信電力）の測定を実施した結果を図14に示す。

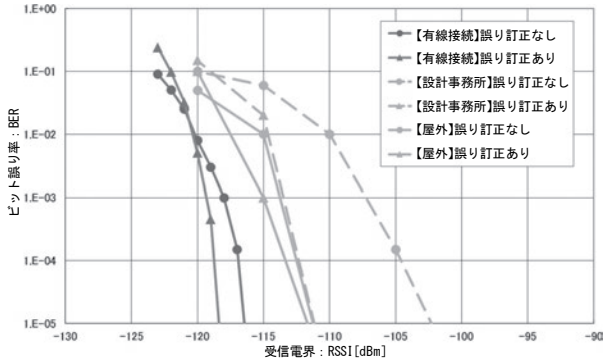

図14　有線接続試験とフィールド試験

図14より、以下の3点を確認できた。

・誤り訂正信号を付加した方が、同じBERに対する必要受信電界が低い。
・事務所内においては、事務機器などから発せられるノイズの影響により、屋外においては建物などの干渉の影響により、それぞれ有線接続時と比較してBERが劣化している。
・事務所内でセキュア無線システムを使用する場合、-111dBmの受信電界を確保するエリアであれば、BERが1×10^{-5}以下となる。

5.3　現業機関での伝搬状況の確認

八王子信号通信技術センター配置の制御装置を用いて、周辺各所へのRSSI、動作許可時間可否の測定を行った。測定場所を図15、測定結果を表1に示す。

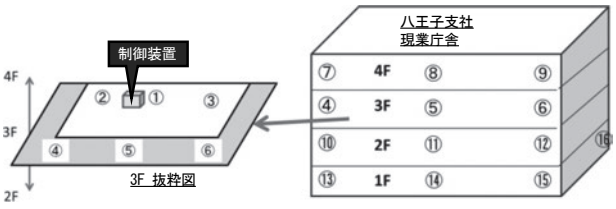

図15　RSSIと動作許可時間可否の測定箇所

表1　RSSIと動作許可時間可否の測定結果

測定ポイント	制御装置側出力：10mW		制御装置側出力：1mW	
	受信電界	通信※1	受信電界	通信※1
①事務所内中央	−	−	-60dBm 以上	○
②事務所内奥（無線機保管場所）	-60dBm 以上	○	-60dBm 以上	○
③事務所内奥（対角の遠い角）	−	−	-60dBm 以上	○
④3F 手前階段	-60dBm 以上	○	-74dBm	○
⑤3F 廊下中央	-65dBm	○	-75dBm	○
⑥3F 奥階段	−	−	-106dBm	○
⑦4F 手前階段	-65dBm	○	-81dBm	○
⑧4F 廊下中央	−	−	-90dBm	○
⑨4F 奥階段	−	−	-101dBm	○
⑩2F 手前階段	-65dBm	○	-90dBm	○
⑪2F 廊下中央	−	−	-91dBm	○
⑫2F 奥階段	−	−	-103dBm	○
⑬1F 手前階段前	-63dBm	○	-102dBm	○
⑭1F 中央	−	−	-107dBm	○
⑮1F 奥階段前	−	−	-114dBm	○
⑯1F 線路側窓側	−	−	-69dBm	○

制御装置に減衰器を挿入し、出力が10mW、1mWで八王子信号通信技術センター（3F）がある4F建ての現業庁舎のすべての箇所で、動作許可時間の更新を行うことができた。

6.　考察

6.1　動作許可信号の輻輳解消に向けて

当社内では50台以上の無線端末を保有する現業機関もあり、スロット数=4、応答スロット固定では、同一スロットで複数の無線端末が衝突する（輻輳）ことになる。

その対応として、応答スロットをランダムに変更することを想定し、動作許可待ちの無線端末数による動作許可信号授受における処理台数の期待値について、スロット数ごとにシミュレーションを行った結果を図16に、その際の処理時間を図17に示す。

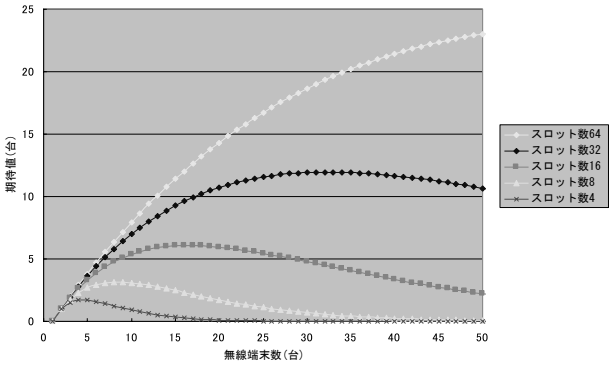

図16　無線端末台数と処理台数期待値

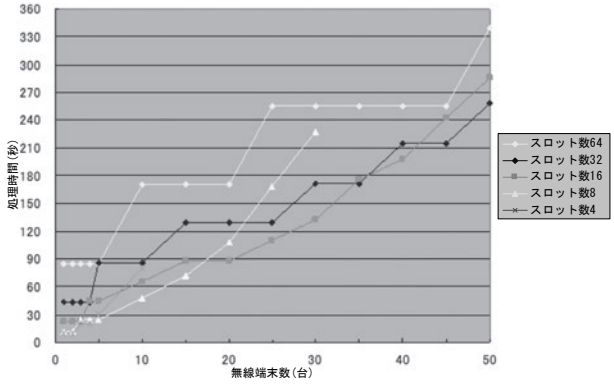

図17　無線端末台数と処理時間期待値

図16からスロット数が増える程、処理できる無線端末数が増えることが確認できる。しかしスロット時間を固定とすると、スロット数が増える程、1回の動作許可信号授受における通信時間も増し、その結果図17のようにスロット数64では最も処理時間を必要とすることが確認できる。

今後スロット時間の削減について検討を行うが、現業機関によって保有する無線端末の台数は大きく異なることから、現業機関に合わせたスロット数の設定が必要となる。

6.2　他社との接続を考慮したネットワーク構成

当社では鉄道の安全運行に関する業務の契約を行っている他社（グループ会社など）に対して、無線局免許の取得や無線端末の貸出を行っている場合がある。それらの無線端末については当社の無線局免許で運用していることから、当社で無線局の管理を行う必要性がある。

他社の無線端末についてもセキュア無線システムへ組み込むことを考慮すると、他社にはJR-IPNetの環境が無いために一般公衆回線を使用する必要がある。当社と他社とのシステム配置構成は以下のように想定される。

・管理装置：当社
・制御装置、無線端末：他社（グループ会社など）

管理装置1台で当社と他社とのセキュア無線システムを担おうとする場合、当社管理装置への社外からの接続については、図18に示すようにVPN（Virtual Private Network）方式や、DMZ（DeMilitarized Zone）方式が検討できる。

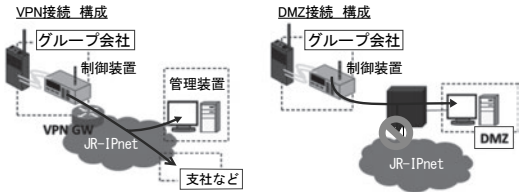

図18　VPNとDMZを用いた場合の各構成

しかしVPN方式を一般公衆回線で行う場合には、当該の管理装置以外の業務用端末に接続できるため、他社の制御装置のウィルス感染した場合、JR-IPNet全体が危険となる。またDMZ方式の場合には、JR-IPNetのファイアーウォール直下に管理装置を設置する必要があり、管理装置自身が外部から攻撃されるおそれがある。

そこで上記の検討から、他社向けの管理装置については、自社向けの管理装置と別に設けることでJR-IPNetへのセキュリティを確保することが適切であると考えられる。

6.3　動作許可時間更新について

現在の動作許可時間更新の仕様では、最後に受信した許可時間によって、動作許可時間を更新する。つまり、意図せず他現業機関から届いた短い動作許可時間で更新することで、想定していた時間ほど無線端末を使用できないことに気づかないおそれがある。

これを防ぐには、他現業機関の制御装置からの電波が受信できないように、設置場所や送信出力を低減させることなどが必要となる。しかし、5.3の表1より制御装置の無線部出力を1mWにした場合でさえ、他フロアの無線端末の動作許可時間を更新できてしまう。そのため同じ建物に異なる現業機関があった場合には、互いに不要な動作許可時間の更新を行うことが想定される。

そのため動作許可時間更新については、
①自箇所からの動作許可時間更新信号のみ受付
②動作許可時間を延長させる場合のみ更新信号を受付

といった案も考えられる。しかし、いずれも装置管理やシステムが複雑化するため、今後運用方法も含めて、導入に当たっての課題整理を進めていく。

7.　おわりに

無線端末に使用許可時間を付与し、不正使用を防止するためのセキュア無線システムの開発を行った。今後は当システムの導入をめざし、機能改善に努める。