

近距離通信技術を利用した利便性の高い 非接触 IC カードシステムの考察

五郎丸 秀樹[†] 池田 実[†] 細田 泰弘[†]

近年、非接触 IC カードを使った入退室システムが増えている。本稿ではこれらのシステムの利便性をさらに向上させる方法として、電界通信に代表される近距離通信技術を組み合わせる方法を提案する。しかしこの方法を既存の非接触 IC カードシステムにそのまま適用すると、応答時間が増加することに起因する種々の課題が生じる。本稿ではこれらの課題の解決方法を提案するとともに、その有効性について実験システムを構築することにより示す。

Study of a Convenient Proximity IC Card System using Short-range Communication Technology

Hideki Goromaru[†] Minoru Ikeda[†] and Yasuhiro
Hosoda[†]

Entry-gate systems are increasingly using proximity IC cards to manage access to restricted areas. To make these systems even more convenient, we propose that they be combined with human-body near-field communication technology, which is a type of short-range communication. However, applying this technology in its present form to existing proximity IC cards results in a variety of problems caused by longer response times. In this paper, we propose a method for solving these problems and describe an experimental system that we constructed to examine its effectiveness.

1. はじめに

近年、職域での入退室サービスにおいて非接触ICカード（以降ICカードとよぶ）の利用が広がり、読み取り機（以降RW（リーダーライタ）とよぶ）にかざすだけで便利にサービスが受けられるようになってきた。本稿では、入退室システムの既存のICカ

[†]日本電信電話株式会社, NTT サービスインテグレーション基盤研究所
NTT Service Integration Laboratories, NTT corporation

ードを利用したシステム（以降ICカードシステムとよぶ）と、最近注目を集めている電界通信技術[1], [2], [3]等による近距離通信システムを組み合わせ、これらを連携動作させることにより、ICカードの利便性を更に向上させたICカードシステムを実現することを目指す。このシステムでは、ユーザはICカードを取り出してRWにかざすことなく、保持しておくだけでサービスを受けることができるようになる。これに加え、既存のICカードシステムがそのまま使えるので、低いコストで実現可能というメリットがある。

ICカードシステムと組み合わせる近距離通信システムについて、ZigBee^{★1}[4], Bluetooth^{★2}[5]等、通信媒体として電波を利用し、ユーザを中心に数メートルの範囲で通信エリアを有するものもある。しかし、ユーザが手や足で接するような、ユーザと密接して通信を実現する電界を用いたものの方がICカードの利用感覚に近く適合性が高いといえる。以上のことから以降では、ICカードシステムと電界通信を利用した近距離通信システム（以降電界通信システムとよぶ）と連携動作させることを想定して議論する。特に既存のICカードシステムへ手を加えずに連携動作させた場合、課題として応答時間の遅延があることを取り上げ、その問題点を示し解決方法として新たなポーリング方式を提案する。

本稿では、まず、2.でICカードシステムと電界通信システムの連携を実現する構成方法を示したのち、3.で連携において生じる課題について述べる。さらに4.で課題を解決するための処理方法について提案する。5.では2.で示した構成、4.で示した処理方法を実装した実験システムについて述べる。

2. 提案する構成方法

2.1 ICカードシステムの概要

ICカードシステムは、図1に示すように、入退室サービスのアプリケーション処理を行う上位機器、上位機器の制御の下でICカードと磁界結合し、ICカードに電力供給、クロック供給、データ授受を行うRW、およびユーザの保持するICカードで構成される。

次に、ICカードシステムの動作概要を図1により示す。ユーザはサービスを受け

^{★1} ZigBee は ZigBee Alliance, Inc. の登録商標です。

^{★2} Bluetooth は米国 Bluetooth SIG, INC. の登録商標です。

る際に IC カードを RW にかざす。すると IC カードは RW が発する磁界から電力とクロックを得て、さらに RW が上位機器からのコマンドに応じて変調した磁界を取り込むことによりコマンドを復調する。このようにして取得したコマンドに対して IC カード内のコントローラでユーザ認証や電子マネー支払いなどアプリケーションに応じた処理を行う。一方、処理結果となるコマンド応答を RW に送り返すため、IC カードは RW が発する磁界に対してコマンド応答に応じた変調を行う。すると RW はこれを取り込んで復調し、上位機器に取得したコマンド応答を伝える。

IC カードシステムは、上記コマンドとコマンド応答の授受を繰り返すことにより、入退室サービス等のアプリケーション処理を進める。特に最初に授受するコマンドとコマンド応答は、ポーリングおよびポーリング応答とよび、RW が発する磁界内への IC カードの進入検出、複数の IC カードの進入が検出された場合において、目的とするカードの選択、ポーリングに引き続きコマンドとコマンド応答を授受する際の通信速度や応答待ち時間などの通信条件を決定する機能を持つ。

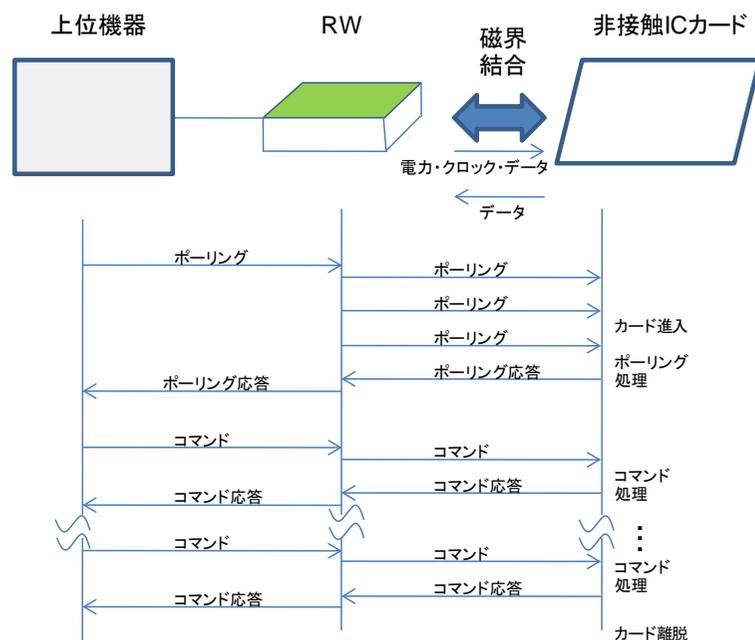


図 1 IC カードシステム

2.2 構成方法

2.1 で述べた IC カードシステムと、電界通信システムを連携動作させる方法について述べる。これは図 2 に示すように、既存の IC カードシステムへ手を加えずに連携動作させた場合の構成であり、IC カードシステムにおける RW と IC カードとの間の磁界結合部分を、電界通信システムに置き換えることにより実現する。以下では RW 側、IC カード側それぞれに電界通信システムを接続する方法について述べる。

<RW 側への接続方法>

図 1 の RW に対して次の機構を追加する。まず、RW が発する磁界からコマンドを復調し、このコマンドをデジタルデータとして電界通信システムに入力する機構(図 2 の矢印①で示す)、次に、電界通信システムからデジタルデータとして出力されるコマンド応答に応じて RW が発する磁界を変調する機構(図 2 の矢印②で示す)を追加する。この機構を容易に実現する方法として、本稿では市販の NFC (Near Field Communication) チップ[6]を活用する方法を提案する。NFC チップは、各種 IC カードに実装されている非接触インタフェースを実現する機能を提供するものであり、磁界を受けて動作する IC カードの機能、磁界を発する RW の機能のどちらの機能も設定で切り替えることにより実現可能である。ここでは IC カードの機能を実現するカードモードに設定し、IC カードの非接触インタフェースとして機能させる。これにより、図 2 に示す 2 つの機構①、②を実現することができる。これを電界通信システムの上位機器側送受信機に接続することにより RW 側への接続が完了する。

<IC カード側への接続方法>

図 2 に示すように、電池で駆動される携帯機器に IC カードを収容する構成とする。ここでは IC カードに次の機構を追加する。まず、電界通信システムからデジタルデータとして出力されるコマンドに応じて磁界を変調する機構(図 2 の③で示す)、次に、IC カードが変調した磁界からコマンド応答を抽出しデジタルデータとして電界通信システムに入力する機構(図 2 の④で示す)を設ける。この機構も RW 側と同様に、NFC チップを RW の機能を実現する RW モードに設定することにより実現する。これにより図 2 に示す 2 つの機構③、④を実現することができる。これを電界通信システムの携帯機器側送受信機に接続することにより IC カード側への接続が完了する。

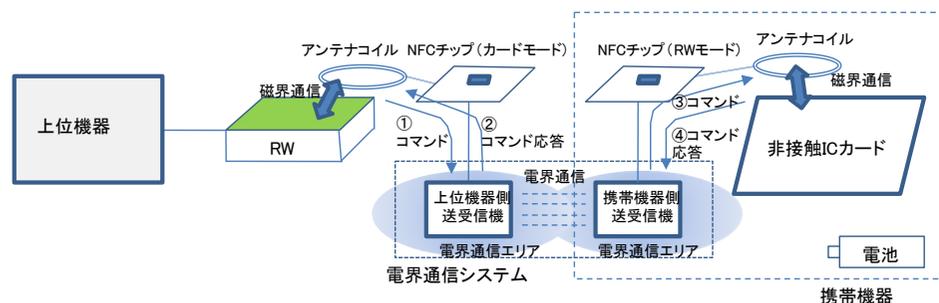


図 2 提案する構成方法

3. 課題

3.1 構成方法を実現する上での課題

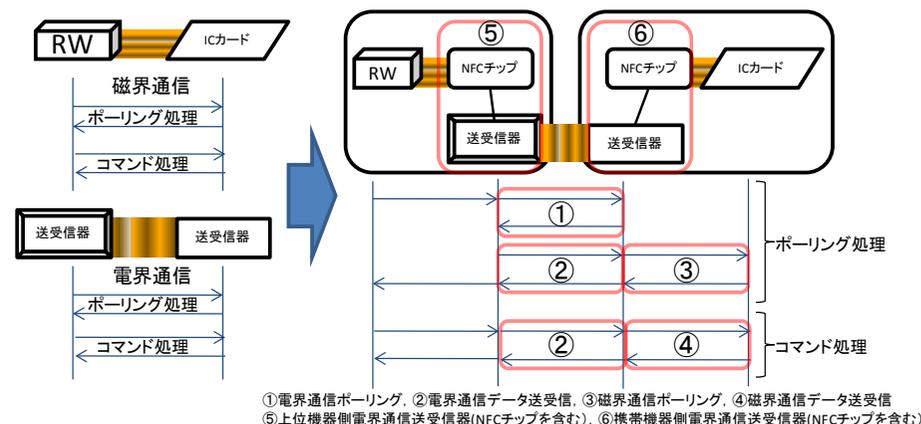
図 2 に示した構成において、ユーザが携帯機器を持って電界通信システムの上位機器側送受信機の電界通信エリアに進入すると、RW が発するコマンドは電界通信により中継され、IC カードに届くため、IC カードを直接 RW にかざすのと同様なコマンドやコマンド応答授受の仕組みを実現することができる。しかしこのシステムを実用的なものとするには次に示すような課題を解決しなければならない。

<課題>

- (1) RW から見ると、電界通信を経由する分、各コマンドの応答時間が増加する(図 3 の①, ②, ③, ④の通信遅延時間, および⑤と⑥の処理時間)。増加の程度によってはサービスの利便性の低下や、RW のタイムアウト時間をオーバーし、RW と IC カードの間の通信自体が成り立たない場合がある。
- (2) 一般的に、RW の磁界通信エリアより電界通信エリアの方が広いので、他のユーザの保持する携帯機器が間違えて応答してしまう可能性がある。
- (3) (2)と同様の理由により、IC カードの狭い通信エリアで担保されていたセキュリティが保証できなくなる。
- (4) 本システムは実験用の構成であるので、実用的なシステムにするには更に詳細を検討しなければならない。

(2), (3)は電界通信システム固有の通信エリアに関する課題であり、他の携帯機器の接近を検知する等、物理的な回避方法を併用しながら解決せざるを得ない。(4)は将来の課題とする。以降では、通信プロトコルの工夫により解決可能な(1)の課題について

検討する。



①電界通信ポーリング、②電界通信データ送受信、③磁界通信ポーリング、④磁界通信データ送受信
⑤上位機器側電界通信送受信器(NFCチップを含む)、⑥携帯機器側電界通信送受信器(NFCチップを含む)

図 3 電界通信を追加することで生じる通信遅延箇所

3.2 ICカード規格と応答時間の課題

ICカードシステムを構成する機器は、相互接続性を向上させるため、国際標準等の規格に基づいて設計されている。表 1 に各種ICカードの規格[7]で定められるポーリング、およびコマンドについて応答時間の許容値の例を示す。

表 1 制限時間例

ポーリング時	コマンド授受時
302.2(μs) [RW からの REQB 最終ビットから、IC カードからの ATQB 開始ビットまでの最大時間]	(256/fs) × 2 ^{FWI} (μs) [fs=847.5kHz, 0 ≤ FWI ≤ 14. 例えば FWI=14 ならば約 4.95(s)]

ポーリングに対するポーリング応答は表 1 に示すタイミングで IC カードは RW に応答する必要があり、これを逸脱すると RW はエラーとして扱う可能性がある。図 2 の構成のように電界通信を経由すると、電界通信の遅延時間が加わるため、IC カードが直接 RW に応答することを前提とした表 1 のタイミングでは間に合わなくなり、エラーとして扱われる問題が生じる。

一方、ポーリング以降のコマンド授受では、規格ではポーリング時にタイムアウト時間を RW と IC カードの間のネゴシエーションにより決定できるようになっている。決定可能なタイムアウト値の最大値は表 1 のように十分大きなものである。電界通信を経由することによる遅延時間の増大を見越したネゴシエーションを行うことにより、

コマンド授受時の応答時間の許容値を大きくすることができるため、エラーとなる問題は回避できる。しかし、各コマンド応答時間は確実に長くなるためサービスが完了するまでの時間も長くなり、サービスの利便性が低下しないか否かの検証が必要となる。

4. 処理方法

3.2 で述べた課題を解決する処理方法について、図 4 に示すタイプ B 非接触インタフェースによる IC カードシステムと電界通信システムを連携させた入退室システムを例として説明する。

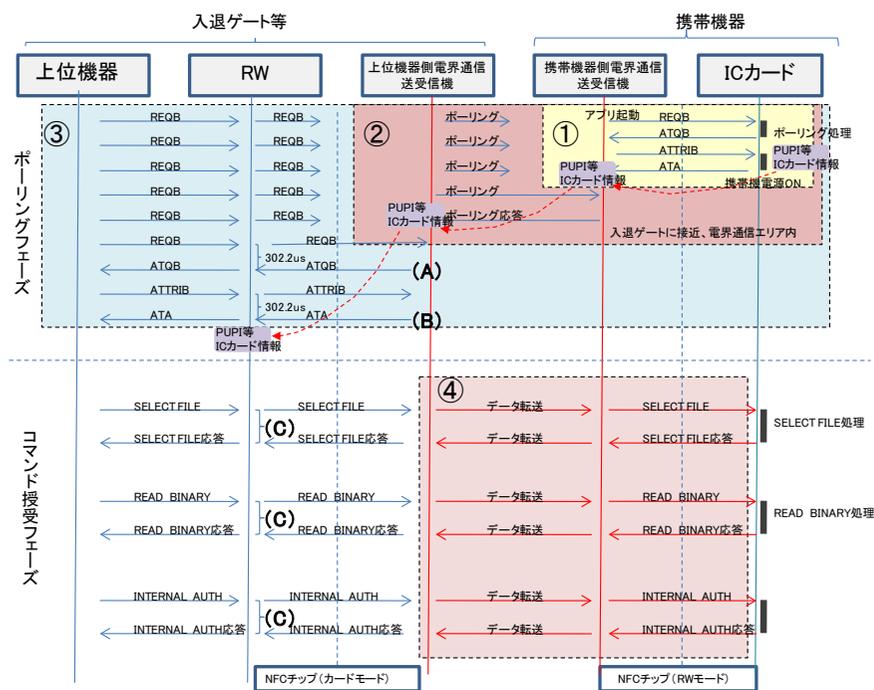


図 4 提案する処理方法

本入退室システムの処理フローは、ICカードを検出し (REQB_{★1}, ATQB_{★2})、ネ

★1 REQB: Request Command, Type B

ゴシエーションを行う (ATTRIB_{★3}, ATA (Answer to ATTRIB)) ポーリングフェーズ、およびICカード上のアプリケーション選択 (SELECT FILEコマンド)、認証処理 (READ BINARYコマンド、INTERNAL AUTHENTICATIONコマンド) を行うコマンド授受フェーズから成り立つ。

4.1 ポーリング処理改善による時間の短縮

ポーリング応答を IC カードの規格で規定される応答時間に返却する方法について述べる。まず、RWが発するREQB, ATTRIBに含まれる情報をあらかじめ携帯機器に登録しておく。この情報を基にRWに代わって前もって携帯機器内部でポーリング、ネゴシエーションを行い、ICカードの情報を読みだしておく(図4のハッチング部分①)。次に、携帯機器が電界通信エリアに進入し、電界通信システムのポーリングを受けると、ポーリング応答の中に、先ほど読み出したICカードの情報を含め、上位機器側電界通信送受信機に伝える(図4のハッチング部分②)。一方、上位機器側電界通信送受信機では、電界通信エリア内に携帯機器が見つかり、かつICカードの情報があったら、RWからのポーリングに対してICカードの情報に基づいて応答する(図4のハッチング部分③)。以上の方法によると、RWからポーリングを受け付けたとき、ポーリング応答に含めるべき情報は上位機器側電界通信送受信機の中に揃っているため、上位機器側電界通信送受信機がICカードと同じ役割を行う。そのため図3の①, ②, ③, ④, ⑤, ⑥の処理がなくなり、表1の応答時間と同じタイミングで図4の(A), (B)で示すATQB, ATAを返却することができる。

4.2 コマンド応答タイムアウト時間の拡大

図4のコマンド授受のフェーズにおいて、電界通信を経由することにより、ICカードを直接RWにかざす場合比べ、SELECT FILE 応答等のコマンド応答が遅れてRWに届くことになる。図4の(C)で示す箇所がコマンド応答時のタイムアウト時間が規定される箇所であり、タイムアウト時間は表1のように規定される。ここで、fsはビットレート、FWIはフレーム待ち時間指数を表す。これらの値は、図4のハッチング部分①の処理において決定され、4.1節で述べたポーリングフェーズにおいて、カード情報として破線矢印のようにシステム内を授受される。そこで、この授受過程のうち(A)で示すATQBを返却する処理において、カード情報のうちFWIの値をより大きい値に書き換える操作を追加する。これにより、RWが意識するタイムアウト時間が拡大され、より応答時間の長いコマンド応答も待ち合わせるように制御することができる。

★2 ATQB: Answer To Request, Type B

★3 ATTRIB: PICC(Proximity Card) selection command, Type B

どの程度 FWI の値を大きくするかについては、電界通信を経由することによる応答時間の増分を実測等で把握することにより、タイムアウトが発生しないような適切な値に書き換える。

4.3 全体処理時間における増分の机上評価

4.2 節で述べた操作により、入退室サービスの処理途中でタイムアウトが発生することなくサービスを提供することができるようになる。しかし、図 4 に示す 3 つのコマンドを実行し終え、サービスが完了するまでの全体の応答時間は、IC カードを直接 RW にかざしたときに比べて長くなる。そこで応答時間が増加してもサービスの利便性が損なわれないか、検証が必要である。ここでは、図 4 のコマンド授受フェーズでの全体の応答時間の増分について机上検証する。

図 4 に示すハッチング部分④が電界通信を経由することにより増加した処理である。この部分で必要とする時間は以下のように分類できる。

- (1) 上位機器側電界通信送受信機の処理時間 (図 3 の⑤)
- (2) 携帯機器側電界通信送受信機の処理時間 (図 3 の⑥)
- (3) 電界通信における通信遅延時間 (図 3 の②)
- (4) IC カードとの通信遅延時間 (図 3 の④)

(1), (2) について、電界通信送受信機では、内蔵するコントローラにおいて、コマンドやコマンド応答を、一旦メモリに蓄積しながら、NFC チップが出力するデジタルデータから電界への変換、およびその逆の変換を行うものとする。コントローラで行う処理はヘッダ付加やエラーチェック処理のみであり、電界への変換処理やメモリへの書き込み、読み出しは通信処理の合間に実行可能であるので通信時間に含める。以上からコマンドとコマンド応答の合計に対する 1 回の処理時間としては 3ms 程度を見込む。コマンドは 3 種類 (SELECT FILE, READ BINARY, INTERNAL AUTH) であるので、(1), (2) の合計の処理時間は $(3\text{ms} \times 3) \times 2 = 18\text{ms}$ となる。

一方、(3), (4) については表 2 と表 3 のように各コマンドの長さ、転送速度から試算すると、(3), (4) の合計の伝送遅延は、 $36\text{ms} + 11.3\text{ms} = 47.3\text{ms}$ となる。

表 2 電界通信における通信時遅延時間

コマンド/コマンド 応答種別	長さ (バイト)	電界通信ヘッダ長 (バイト)	ビットレート (kbps)	通信時間 (ms)
SELECT FILE	30	100	200	6.5
SELECT FILE 応答	10	100	200	5.5
READ BINARY	10	100	200	5.5
READ BINARY 応答	20	100	200	6.0
INTERNAL AUTH	30	100	200	6.5
INTERNAL AUTH 応答	20	100	200	6.0
				36.0

表 3 IC カードとの通信遅延時間

コマンド/コマンド 応答種別	長さ (バイト)	ビットレート (kbps)	通信時間 (ms)
SELECT FILE	30	106	2.8
SELECT FILE 応答	10	106	0.9
READ BINARY	10	106	0.9
READ BINARY 応答	20	106	1.9
INTERNAL AUTH	30	106	2.8
INTERNAL AUTH 応答	20	106	1.9
			11.3

< 試算の条件 >

- 電界通信のビットレート 200kbps, ヘッダ長 100byte
- IC カード通信のビットレート 106kbps
- 1 バイトのデータに対して開始ビットと終了ビットを付けるため、1 バイトに対し 10bit の伝送量とする。

< 試算結果 >

(1), (2), (3), (4) の合計の応答時間は $18\text{ms} + 47.3\text{ms} = 65.3\text{ms}$ と試算され、約 70ms の増加となる。約 70ms 応答時間が増加する結果となるが、一般的な入退室サービスにおいては、サービスの利便性を大きく損なうものではないと予想される。

これは IC カードシステムとは違い、電界通信の場合は応答時間の増分を運用でカバーできるためである。例えば上位機器側電界通信送受信機のアンテナを入退室ゲートの直前の床に埋め込み、その上を通過するときに認証することで IC カードシステムよりも早目に認証が可能であり、その距離を調整することで対処できるからである。

5. 実験システム

2.2 節で示した IC カードシステムと電界通信システムの連携方法、および 4.1 節で述べたポーリング応答方法の実現性を実際に確認するため、プロトタイプとして実験システムを製作した。ここでは電界通信システムとして RedTacton[3]を利用した。実験システムの構成を図 5 に示す。

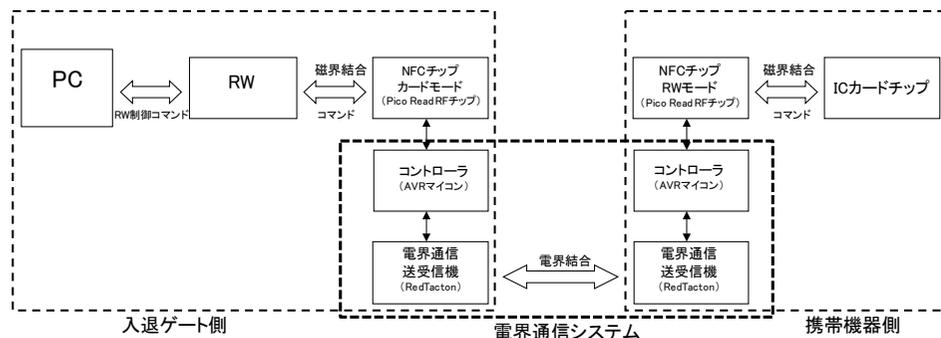


図 5 実験システムの構成

図 5 に示す入退ゲート側において、RW が発する磁界から IC カードコマンドを復調すること、および携帯機器側で RedTacton を介して伝送された IC カードコマンドを磁界によって IC カードに伝えることを実現する NFC チップとして、PicoRead RF チップ[6]を利用した。また AVR マイコンによるコントローラにより PicoRead RF チップおよび RedTacton の電界通信送受信機の制御を行い、IC カードシステムと電界通信システム間の IC カードコマンドの受け渡しを行った。

この構成により、図 5 に示す PC から投入された IC カードコマンドが、RedTacton を経由して携帯機器側に転送され、IC カードチップで処理されること、逆に処理結果がレスポンスとして、RedTacton を経由して RW に戻されることを、IC カードコマンド実行の結果、PC に表示されるレスポンスにより確認した。

また、携帯機器側の電源投入時に携帯機器側のコントローラから IC カードチップにポーリングを行い、IC カード情報を取得するようにコントローラのプログラムを変更する等、図 4 のポーリング応答方法を実現するように各コントローラのプログラムを変更した。これを実行することにより、単純に電界通信を経由したとき(図 3 の①, ②, ③, ④, ⑤, ⑥の合計)は 30ms 近くかかっていたポーリング応答時間を、表 1 に示す時間に合わせると 100 μ s 以下の応答時間まで短縮できることを確認した。

以上述べた実験システムにより、提案した方法が実現可能であることを確認した。

6. おわりに

本稿では、さらに利便性の高い IC カードシステムを実現する方法として、既存の IC カードシステムを近距離通信のひとつである電界通信と連携させる手法について述べた。既存の IC カードシステムに本稿で提案した機構を追加することにより実現可能であるので、安価に実現できることに加え、既存の IC カードもそのまま利用できるというメリットがある。しかしこのシステムを実用的なものとするには、入退室サービスの運用時を想定したデータを収集して更に問題点を洗い出すと共に、今後 3.1 節で述べた、本稿では解決方法について取り上げなかった課題についても解決していく必要がある。

参考文献

- [1] IEEE P802.15 “Wireless Personal Area Network”,
<https://mentor.ieee.org/802.15/dcn/10/15-10-0245-04-0006-tg6-draft.doc>
- [2] “アルプス電気、人体通信向け新モジュール量産”,
<http://www.nikkan.co.jp/news/nkx0320100629aaag.html>
- [3] ”特集 ヒトとモノ,ネットワークをつなぐヒューマンエリアネットワーク技術の動向とビジネス展望”,NTT 技術ジャーナル,Vol.22,No.1,2010.1.
- [4] ZigBee Alliance, <http://www.zigbee.org/>
- [5] Bluetooth.org, <https://www.bluetooth.org/apps/content/>
- [6] Contactless Reader Chips PicoRead ,Inside Secure,
<http://www.insidesecond.com/eng/Products/Smart-Card-Readers/Contactless>.
- [7] ISO/IEC 14443 “Identification cards -Contactless integrated circuit(s) cards- Proximity cards”,
 ISO/IEC,2006.