技術基礎講座

【非接触ICカード技術】

他の通信システムと同様に，非接触ICカードシステムにおいてもリーダライタ・カード間の通信に規約があります．また，接触式ICカードにはない，非接触ICカード特有の処理も存在します．ここでは，リーダライタとICカード間における通信規約の説明に加え，非接触ICカード特有の処理についても触れます．

非接触ICカードシステムの主な要件

鉄道改札や入退管理システムなど多くの非接触ICカードシステムでは，目的の非接触ICカード（カード）1枚のみをリーダライタにかざします．しかしながら，リーダライタの周囲には他のカードが存在する場合もあります．その場合でも，読み書き対象となるカードとのみ通信できるよう，カードを正しく識別しなければなりません(1)．

また，通信経路上のデータが傍受して解読され，データ改ざん・なりすましなどが行われるというリスクを，情報通信システムでは無視できません．カードシステムにおいても，データをより安全に読み書きできる方法として，暗号を用いた通信が重要になりつつあります．

非接触ICカードシステムにおける通信プロトコル

他の通信システムと同様に，カードシステムにおいても，リーダライタとカード間での通信規約（プロトコル）が定められています．通信シーケンスは，リーダライタと目的のカードとの通信路を設定する「初期応答」と，アプリケーションに応じた情報の授受を行う「活性状態」とで構成されます．通信シーケンスの基本的な構成は，まずリーダライタがコマンドを送出し，それを受けてカードが応答を返すように定められています（リーダトークファースト）．また，リーダライタ→カード，カード→リーダライタの両方向とも，データはシリアルで伝送されます．リーダライタとカード間での基本的な通信シーケンスを，1枚のカードを使用する場合を例に説明します（**図1**）．

■初 期 応 答

まず，カードがリーダライタの磁界に入ると，ICチップに電源が供給され，カードは，リーダライタからの通信路の設定要求（リクエストコマンド）を待機する状態になります．次に，リーダライタからリクエストコマンドが送信され，カードは応答を返します．これにより，リーダライタの通信エリアに存在するカードが認識されます．その後，リーダライタは，認識したカードとの間でパラメータを交換し，通信速度などの条件を相互に確認します．これを経て，活性状態に遷移します．

初期応答の処理方法は，カードのタイプにより異なります．初期応答に関する標準規格ISO/IEC14443-3では，タイプAとタイプBの2方式 (2) が規定されています．

■活 性 状 態

活性状態では，「初期応答」で認識したカードを選択し，リーダライタからのコマンドに対するカードからのレスポンスを繰り返すことを基本としています．初期応答と異なり，活性状態では，ISO/IEC14443-3のタイプに関係なく，接触ICカードと同様の通信プロトコルを用います．この通信プロトコルには，キャラクタ単位で伝送する「キャラクタ伝送」およびブロック単位で伝送する「ブロック伝送」の2つが規定されていますが，ここでは，ブロック伝送の概要を説明します．

伝送ブロックにはIブロック（情報ブロック）・Rブロック（受信準備完了ブロック）・Sブロック（管理ブロック）の3種類があり，データの通常の読み書きには，Iブロックを使用します．

伝送ブロックは，先頭フィールド，情報フィールドお

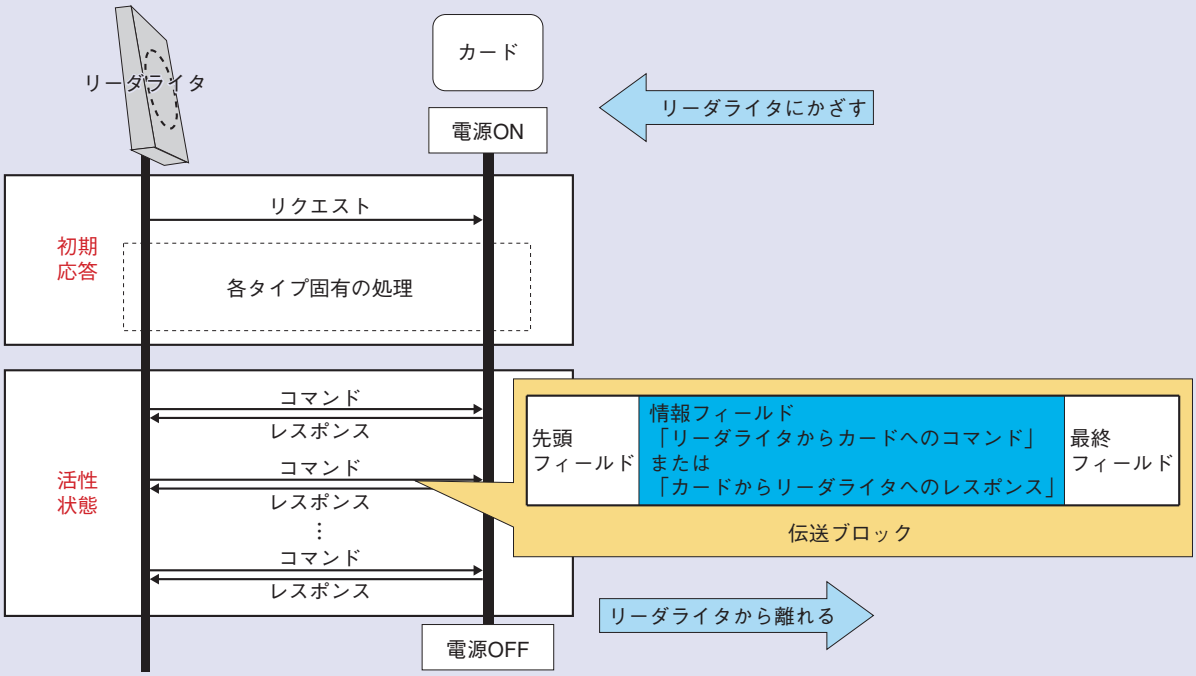


図１　非接触ICカードシステムにおける通信シーケンスの概要（カード１枚使用時）

よび最終フィールドの３つで構成されます．先頭フィールドには，全体の伝送をコントロールするための情報が入ります．コマンドおよびレスポンスは，情報フィールドに挿入します．また，データのエラーチェックができるよう，最終フィールドとしてエラー検出コードが付加されます．

伝送ブロックを受信したリーダライタ・カードは，伝送ブロックの情報フィールドを解釈して，所定の処理を行います．

また，アプリケーションに応じた情報の授受以外に，リーダライタとカードとの間で通信条件の設定等も行います．これにより，本通信プロトコルを実装した製品どうしを組み合わせたシステムでも円滑な通信が可能となります．

アンチコリジョンは複数のカードの“交通整理”

複数のカードを使い分けるアプリケーションでは，「初期応答」で認識した複数枚のカードを１枚ずつ選択して読み書きを行います．初期応答において，リーダライタに複数のカードをかざすと，リクエストコマンドに対して複数のカードが同時に応答しますが，リーダライタ側でカードを正しく識別できない状態が発生します．この状態を「コリジョン」と呼び，それを防ぐ処理（アンチコリジョン）が必要となります．次に，現在広く用いられている２つのアンチコリジョン方式について説明します[(3)～(5)]．

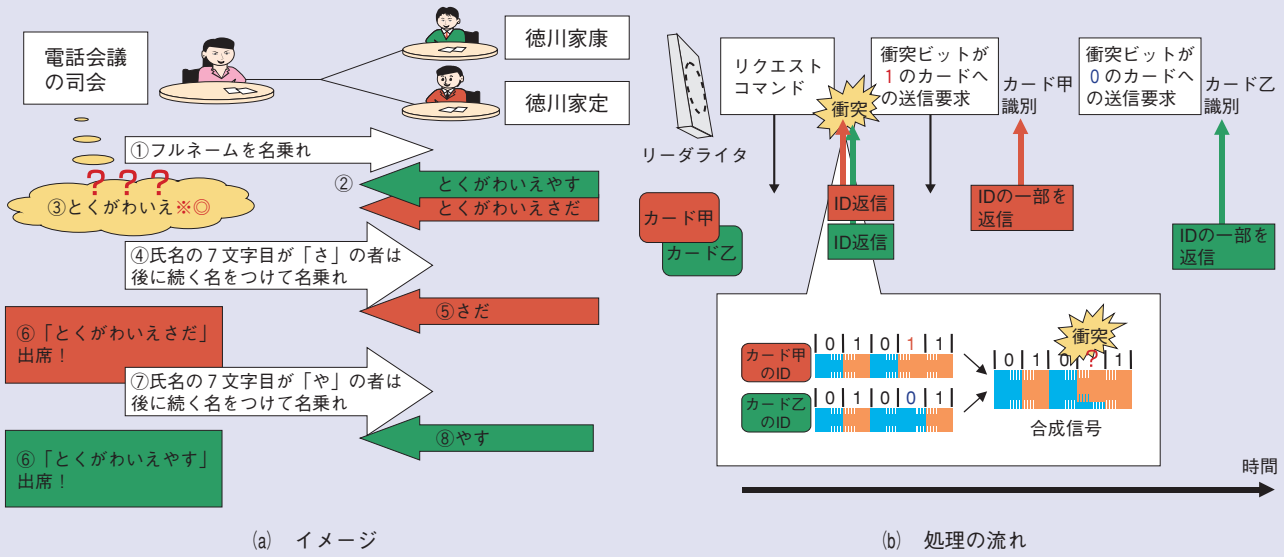
■ビットコリジョン方式

この方式は，電話会議に同姓の社員が出席し，司会の点呼に対し，フルネームで返事をするというルールで出席者を確認していく作業に似ています（**図２**(a)）．

電話会議の司会が，フルネームを名乗るよう指示すると（①），２人が同時に同じ速さで返事します（②）．この時点では，司会には，「とくがわいえ」で始まる社員が出席していることは聞き取れますが，名前の一部が混ざって聞こえるため，フルネームを区別できません（③）．そこで，司会は，区別できなかった文字以降について条件をつけて名乗らせます（④）．図２(a)の④の条件では，徳川家定さんだけが「さだ」と返事します（⑤）．これによって，司会は，徳川家定さんの存在を確認できます（⑥）．以後，名乗らせる条件を変えて指示を繰り返し，出席者全員を特定します（⑦）．

このイメージを非接触ICカードシステムに置き換えると，図２(b)のような流れになります．

・カード甲・乙とも，リーダライタからのリクエストコ



(a)　イメージ　　(b)　処理の流れ

図２　ビットコリジョン方式によるカード識別

マンドを受信すると，同時にIDを返信する．

・リーダライタでは，送信されてきたビット列を順に受信し，“0/1”を判別する．最初の３ビット目までは“010”を正しく受信できるが，４ビット目は図２(b)の「合成信号」のように潰れるため，コリジョンが発生したことを検知する．

・リーダライタは，確定した３ビット“010”およびコリジョンの発生した第４ビットに“1”を指定して，パターン“0101”に一致するIDを持つカードだけが応答するように要求する．このとき，カード甲のみが応答を返す．

・IDの最終ビットまで衝突がなければ，リーダライタは受信したID全ビットをカード甲に送信し，カード甲は自身のIDに一致することを確認して応答する．これにより，リーダライタはカード甲を識別したこととなる．

・リーダライタは，確定した３ビット“010”および第４ビットに“0”を指定して，パターン“0100”に一致するIDを持つカードだけが応答するように要求する．このとき，カード乙のみが応答を返す．

ビットコリジョン方式は，ISO/IEC14443-3 タイプAで標準化されています．この方式では，ID全体ではなくビット単位で衝突の有無を検出しますので，比較的高速に識別できるという特徴があります．ただし，同一IDのカード複数枚がリーダライタにかざされた場合にはリーダライタ側は識別できないため，カードメーカ間で重複しないIDの付与が必要となります．

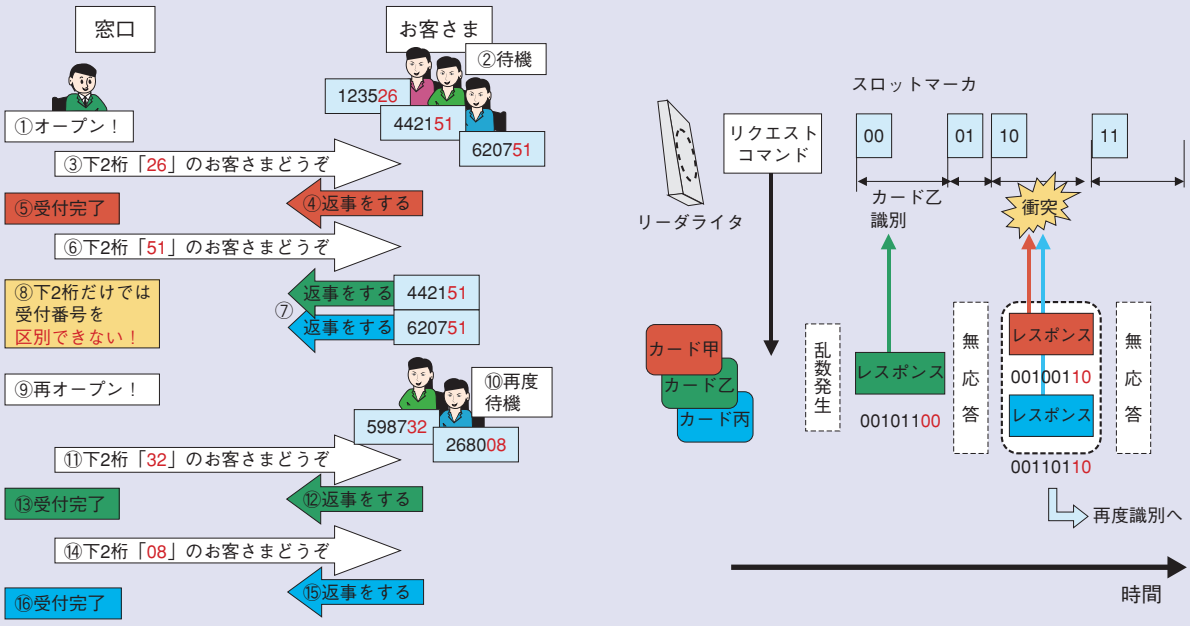
■スロットマーカ方式

この方式は，ランダムな数字が印字される受付番号札を持ち，窓口から呼び出される受付番号が，手許の札番号の一部に一致した場合に返事することに似ています(**図３**(a))．

まず，窓口が開くと(①)，お客さまは受付番号札を持って待機します(②)．次に，窓口は受付番号下２桁を間隔をあけて読み上げていきます(③)．お客さまはその番号を聞き，自分の持っている札番号に一致したとき，窓口に対して返事します(④)．ある時間枠で，下２桁が同じで他の桁が異なる他のお客さまも同時に返事した場合(⑥，⑦)，窓口ではそれぞれの札番号を聞き分けられない(⑧)ため，その時間枠での受付をあきらめます．受付番号下２桁の読み上げをすべて終えて，再度窓口を開けます(⑨)．受け付けられなかったお客さまは，再度，番号札を持ちます(⑩)．札番号はランダムに印字されますので，今度は，下２桁が互いに異なることが期待できます．以後，最後のお客さまが受け付けられるまで，上に述べた応対が繰り返されます(⑪～⑯)．

このイメージをカードシステムに置き換えると，図３(b)のようになります．

・リーダライタは，使用するスロット数(ここでは，スロット番号00，01，10，11の４個)を含めた



⑷ イメージ　　⑸ 処理の流れ

図3　スロットマーカ方式によるカード識別

リクエストコマンドを含めてカードに送出する．

・各カードは，受信したリクエストコマンドに含まれるスロット数に基づき，ランダムに応答するスロット番号を選択する．

・リーダライタは，スロットを示すコマンド（スロットマーカ）4個を順番に送信し，カードからの応答を待つ．

・スロット番号“00”を指定したスロットマーカに対しては，カード乙が応答する．リーダライタはこの応答を確認してカード乙を識別する．

・スロット番号“01”に対して無応答なので，リーダライタはその次のスロット番号“10”を指定する．このとき，カード甲・丙が応答するが，信号が重なっているため，リーダライタはコリジョンが発生したことを検知し，カード識別を保留する．

・保留していた上記2枚のカードを識別するため，リーダライタはリクエストコマンドを再送出する．今度は，2枚のカードが生成する乱数が互いに異なり，別々のスロットで返信することが期待できる．以後，リーダライタは，すべてのカードを識別するまでこの処理を繰り返す．

スロットマーカ方式は，ISO/IEC14443-3タイプBで標準化されています．この方式では，スロットの時間は任意ゆえ，該当カードが応答しなければすぐ次のスロットに進めるため，識別にかかる時間の短縮が期待できます．また，スロット数を多くすればするほど，応答するスロットの分散が期待できるため衝突を防げるという特徴があります．ただし，スロット数を多くした分，カードをすべて識別できるまでの時間が長くなることがあります．

なお，スロットマーカ方式と似た方式で，スロット時間が均等な「タイムスロット方式」もあります．仕様の詳細は両者で異なりますが，FeliCaカードや，ISO/IEC14443-3のAnnex-Cで標準化されているアンチコリジョンはタイムスロット方式を用いています．

以下では，カードデータの読み書き機能以外に非接触ICカードシステムが対応している機能のいくつかを紹介します．

待ち時間変更要求

カードシステムでは，初期応答の時点で，リーダライタからコマンドを出した後の待ち時間（FWT：Frame Waiting Time）をICカードとあらかじめ示し合わせます．リーダライタは，FWTを超えても応答がなかった場合，

タイムアウトと判断します．このFWTを延長できるよう，カードからリーダライタを制御する機能（Sブロックを用いたフレーム待ち時間延長要求）があります．この機能を用いることにより，あらかじめ設定しておいたＦWTを延長することができます．これにより，タイムアウトが想定されるときにFWTを延長させるように制御できますので，長いデータの読み書きやカード内で処理時間のかかる情報の授受にも対応できます．

チェイニング

リーダライタとカードは，それぞれが一度に受信できる最大フレーム長をあらかじめ示し合わせておきますが，そのサイズを超えるデータを読み書きする場合もあります．このような場合に，ISO/IEC14443-4で規定されている「チェイニング機能」を使うことができます．その例として，一度に受信できるフレーム長が８バイトのカードに，12バイトのデータを送信する場合について，**図４**を用いて説明します．

・リーダライタは，先頭フィールドおよび最終フィールドのバイト長も考慮して，送信対象のデータを分割する．
・分割データをカードに送信する際，先頭フィールドには，直後に送信するデータとの関連を示す情報を含める．
・リーダライタは，カードからの受信確認（Rブロックを使用）を待って，次の分割データを送信する．
・分割データ（最終）をカードが受信すると，カードは分割データを結合して元のデータを解釈し，所定処理を行う．その後，最初のコマンドに対するレスポンス（Iブロックを使用）を返す．

分割数を少なくするためにフレーム長を長く取りすぎると，カードをかざしている間の磁界の変動等により，通信エラーとなることが多くなります．逆に，送信データを細切れにしすぎると，分割データの送信・受信確認の切り替え回数が増え，データ送信を完了するまでの時間が長くなってしまいます[(4)]．

暗号を用いた通信

データをより安全に読み書きする方法として，カードシステムには，セキュアメッセージングに関するいくつか

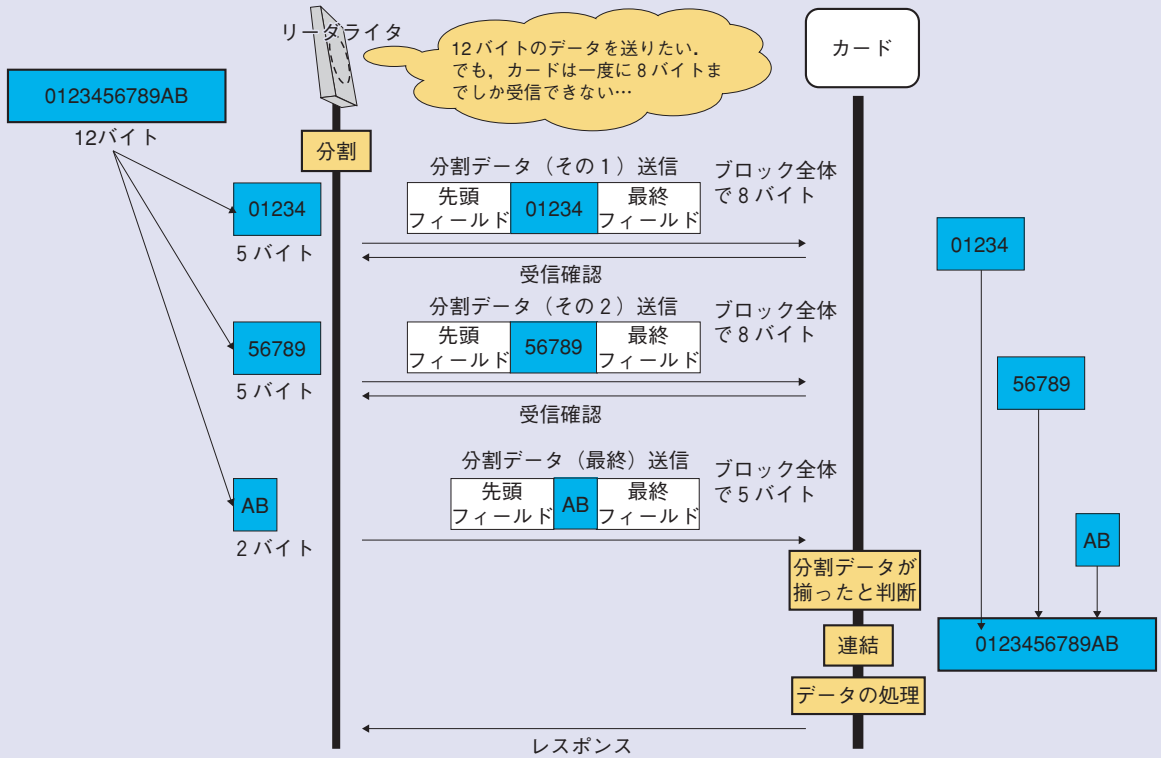


図４　チェイニングの流れ

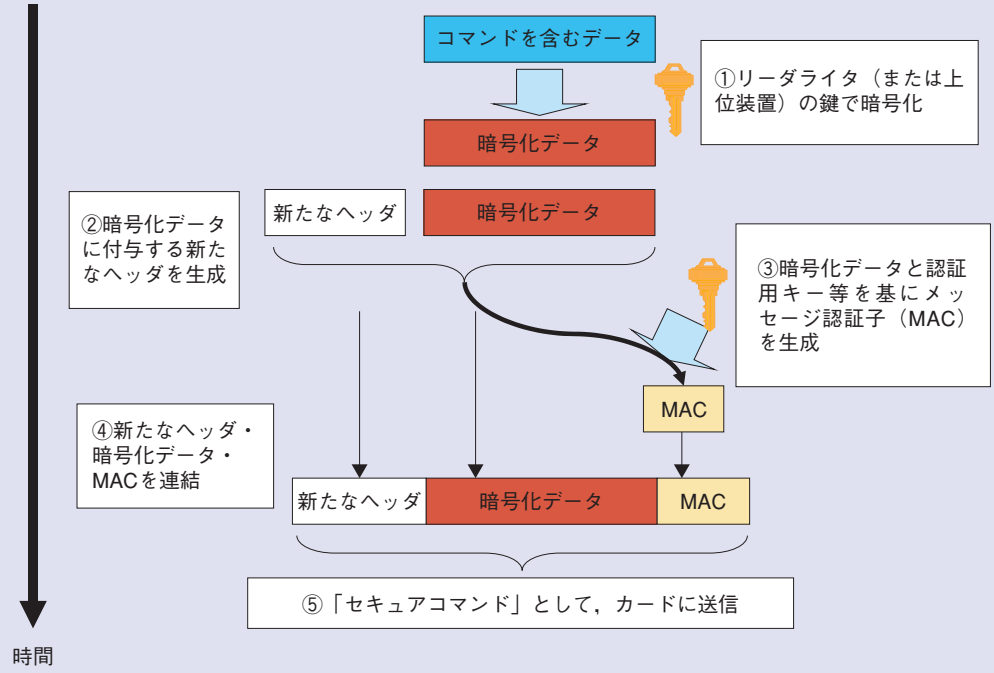


図5　セキュアメッセージングの流れ

の手順が規定されています．その一例として，リーダライタにおける，セキュアコマンドの生成からカードへの送信に至る流れについて，**図5**を用いて説明します．

・カードへのコマンドを含むデータを暗号化し，これを暗号化データとする（①）．
・暗号化データに付与する新たなヘッダを生成する（②）．
・①で生成した「新たなヘッダ」および「暗号化データ」のMAC（Message Authentication Code）を生成する（③）．
・②で生成した「新たなヘッダ」，①で生成した「暗号化データ」，および③で生成したMACを連結し（④），「セキュアコマンド」としてカードに送信する（⑤）．

一方，カードは，受信したセキュアコマンドのデータ部分を基にMACを生成し，リーダライタから送信されてきたMACと一致することを確認します．次に，受信したセキュアコマンドの「暗号化データ」を復号し，元の「コマンドを含むデータ」を解釈し，そのコマンドに応じた処理を行います．

以上により，セキュアメッセージングを用いた通信では，読み書き対象となるデータの保護や改ざん防止を担保することができます．その反面，読み書き対象でないデータが付加されることによる送受信データ全体の増加，および，カードやリーダライタ（または上位装置）内での暗号化および復号処理ゆえ，読み書きに要する時間は，セキュアメッセージングを用いない場合に比べて長くなります．このため，セキュリティと高速処理のトレードオフを考慮する必要があります．

■参考文献

(1) 技術基礎講座：“非接触ICカード技術 第2回 サービスに応じた非接触ICカードとリーダライタ，”NTT技術ジャーナル，Vol.20,No.2,pp.75-78，2008.
(2) 技術基礎講座：“非接触ICカード技術 第3回 非接触ICカードとリーダライタとのインタフェース（物理レイヤ），”NTT技術ジャーナル，Vol.20, No.3, pp.81-85, 2008.
(3) K. Finkenzeller：“RFIDハンドブック第2版，”日刊工業新聞社，2004.
(4) 苅部：“非接触ICカード設計入門，”日刊工業新聞社，2005.
(5) 苅部：“トコトンやさしい非接触ICカードの本，”日刊工業新聞社，2003.

◆問い合わせ先
NTTサービスインテグレーション基盤研究所
ICカードサービス推進プロジェクト
E-mail　sd-info@lab.ntt.co.jp

このコーナで取り上げて欲しいテーマをE-mailで編集部までお寄せください．
●㈳電気通信協会内　NTT技術誌事務局　E-mail　jimukyoku2008@tta.or.jp