NTag424DNA対応
13.56MHzリーダ／ライタ
コ マ ン ド 説 明 書

型番：ＨＦ－ＣＬ０６ＢＵ２(DNA)

２０２５年　１月１０日

第１版

大信機器株式会社

大信機器株式会社

本　　社　〒５５６－０００５
大阪市浪速区日本橋５－１－１９
（営業部）　ＴＥＬ　０６－６６４１－７６３３（代表）
ＦＡＸ　０６－６６４１－７６３７

安全のための基本的注意事項

取り扱いを誤りますと、本製品に搭載しているコンデンサーやICチップなどが過熱し、**怪我**をしたり、**火災**に至る恐れがありますので、下記の注意事項をお守り下さい。

・異常な臭いがしたり、過熱したりしたときは使用しないで下さい。
・電源電圧及び極性を間違わないで下さい。
・結露しているときは電源を入れないで下さい。
・傷んだ電源ケーブルを使用しないで下さい。
・異物を落としたり、液体などを製品にこぼさないで下さい。
・落としたりぶつけたりしないで下さい。
・分解しないで下さい。
・基板に水や異物が付いたときは、使用を中止して下さい。
・電源端子部（＋とー）に金属物（ネックレスやヘアピンなど）を接触させないで下さい。
・油煙・湯気・湿気・ほこりなどが多いところ、振動が激しいところに置かないで下さい。
・お手入れの際や長期間使わないときは、安全のため、電源をお切り下さい。
・高温になる所や夏場の密閉した自動車等の車両内などや極端に寒いところに放置しない。
・防虫剤などの薬品やゴム、ビニール製品に長時間接触するところに放置しないで下さい。
・砂が掛からないようにして下さい。

ご使用にあたって

・本製品を使用される場合は、ご購入者様の責任において安全性を十分考慮した設計及びエージング処理など、ご購入者様の装置としての出荷保証をお願い致します。

本製品の用途について

・本製品は一般電子機器用に使用される目的で製造された製品で、高い信頼性を必要とされる用途の使用は、信頼性及び安全性維持の為に適切な処置を講じた上でご使用下さい。

通信設備を有する機器のご利用にあたって

本機は、一般利用可能なＩＳＭ帯域である１３．５６ＭＨｚの電波を利用した通信設備を有しているＲＦタグ用リーダ／ライタです。そのため、使用する用途・場所によっては混信が発生することがあります。この混信による影響を少なくするために、導入に際しては相互に事前に確認されることをお願い致します。また、電波天文や医療機器等に影響を与える恐れもあり、このような環境での使用については特にご注意して下さい。

心臓ペースメーカをご利用の方へ

本リーダ／ライタは RF タグと電波で交信をするため、使用場所および用途によっては医療機器に影響を与える恐れがあります。

- 電波に影響を受ける恐れのある精密医療機器の周辺では、ご使用を控えて下さい。特に医療機関等の指定した使用禁止場所では、必ず電源を切って下さい。
- 植え込み型心臓ペースメーカ及び植え込み型除細動機器等をお使いの方ご自身、もしくはお使いの方が直近に居られる場合は、本リーダ／ライタのアンテナ部をそれらの機器の装着部位から 22cm 以内に近づけない様ご注意下さい。

尚、本製品のご使用に際しましては、（社）日本自動認識システム協会で作成しました「運用ガイドライン」を確認の上、お取扱いお願い致します。

目　次

１．はじめに

- 本書は、13.56MHz ISO14443 リーダ／ライタ HF-CL06BU2(DNA)のコマンドについて説明しています。以降、本リーダ/ライタを R/W と略記します。

- R/W は「NTag424DNA(以降 DNA と略記します)にセキュリティ付の NDEF を書込む」ことに特化しており、現在、他の ISO14443 タグへのアクセスコマンドは一部しか組込まれていません(CPU に余裕がある為、今後検討します)。

- R/W は、DNA に対して、①URL をセキュリティ付 NDEF として書込、②DNA の Key 設定や変更、③NDEF への書換禁止の設定、等を行います。

- 弊社 R/W は通常、コマンド･パラメータの区切り文字として“,”(カンマ)を使用しますが、本 R/W は URL をコマンドパラメータとして発行する為、URL に使用可能文字のカンマの代わりに“<”を区切り文字として使用します。

- セキュリティ付 NDEF が登録された DNA を読出すと、応答される URL に「UID とカウンタを暗号化した文字列(16By:32 文字)」「照合用 CMAC(8By:16 文字)」が応答されます。
  詳細は本文に記しますが、本書では前者を「ミラー」、後者を「CMAC」と略記します。

１－１　対応記憶媒体

対応する記憶媒体は ISO14443 のみで、下表の様に対応しています。

記憶媒体	対　応　動　作
NTag424DNA	Key の設定･変更 NDEF 書込 認証 NDEF セキュリティ設定 書換禁止設定
Standard シリーズ	スキャンのみ
Desfire	
Ultralight シリーズ	スキャン 全件読出
NTag203	
21x シリーズ	

※ ISO15693,FeliCa Lite-S 等の対応は出来ません(弊社製の他のリーダ/ライタをご利用下さい)。
※ 本書では、DNA を除く NTag シリーズ、及び、Ultralight シリーズを、「UL 系タグ」と総称します。
※ 上表にて「全件読出」に対応しているタグについては、他の機能の対応を検討しています。

２．コマンド概要

コマンドの入力は、全て ASCII コードを用います。コマンドの中の数値は 16 進数を ASCII で入力して下さい（例：10 進数の 15 を 16 進数で登録する場合、値は 0F となるので、“0” “F”を ASCII 即ち 30h 46h と発行して下さい）。

応答されるエラー番号は下記の通りです。

エラーコード	内　　容	その他
ER00	カード無し	
ER01	認証エラー	
ER02	読出失敗	
ER03	書込失敗	
ER04	コマンドエラー	全コマンド共通

※　エラー番号は弊社製品の Mifare リーダ／ライタと合わせています。以下に記しますコマンドと異なる文字を送信した場合 及び 書式を間違えた場合は、コマンドエラーが応答されます。

本 R/W のコマンドは、大別して「共通コマンド」、「ISO14443 コマンド」、「DNA 専用コマンド」の 3 種があります。それぞれに分類されるコマンドは、以下の通りです。

共通コマンド

「V:バージョン情報」
「M:モード切替」
「B:ブザ制御」(ブザ付きの機種のみ有効です)

ISO14443 コマンド

標準コマンドを継承するものは、現在、以下の 2 種類です。
「XX･XS:スキャン系コマンド」
「RU:UL 系タグ全読出コマンド」

本 RW には、新たに「上位側で発行した文字列を直接タグに送信し、そのレスポンスを上位に応答」する「t:スルーコマンド」を新設しています。

※ 今後、既存のコマンドへの対応等も、検討しています。

DNA 専用コマンド

[DNA]の Key 変更、DNA への NDEF 書込及び設定等を行います。
コマンドコードは NDEF の頭文字「N」より始まります。
詳しくは、後述の「3-3 DNA 専用コマンド」を参照下さい。

３．各コマンド

３－１．共通コマンド

V：バージョン情報

ファームウェアのバージョンを応答します。

コマンドモード			書　式
バージョン情報	コマンド		V[CR]
	レスポンス	ブザ無	NTag424DNA V16.01[CR]
		ブザ付	NTag424DNA VB16.01[CR]
PC モード			書　式
バージョン情報	コマンド		V
	レスポンス	ブザ無	NTag424DNA V16.01[CR][LF]
		ブザ付	NTag424DNA VB16.01[CR][LF]

M：モード切替

各コマンドのレスポンス形式の切替を行ないます。

● レスポンス形式の設定

レスポンス形式には、主としてプログラムで制御する為のコマンドモードと、画面に表示した時に見やすいよう表示位置を調整した PC モードの２種類があります。

コマンドモード時には、他のほぼ全てのコマンドの末尾にデリミタの[CR]が必要となります。

コマンド・PC モード共通		書　式	コマンド・PC モード共通		書　式
コマンドモードにする	コマンド	M+	PC モードにする	コマンド	M-
	レスポンス	+OK[CR]		レスポンス	-OK[CR][LF]

※　モード切替コマンドは、どちらのモードから行なっても、デリミタの[CR]は不要です。

※　起動時のレスポンス形式は、コマンドモードに設定されています。

B：ブザ制御コマンド

本コマンドは、USB リーダ／ライタ等の様にブザを実装しているリーダ／ライタのみ有効で、他の機種ではコマンドエラーレスポンスが応答されます。

※ ブザ鳴動の単位は約 0.1 秒で数 ms の長短がありますが、以降 0.1 秒単位として記します。

ブザの鳴動は、自動と手動の２種類のモードをコマンドで選択できます。

本書に於いて、「自動」から「手動」への切替を「設定（セット）」、その逆を「解除(リセット)」と表現します。

ブザの鳴動は、設定／解除により、下表の様になります。

設定／解除	状　　態	鳴　　動
設定時	タグアクセス成功時	無音
	ブザ鳴動コマンド発行時	コマンドにより鳴動
解除時	タグアクセス成功時	0.1 秒 鳴動
	ブザ鳴動コマンド発行時	コマンドエラー

BS：ブザコマンド設定

ブザ鳴動コマンドを有効にします。タグアクセス成功時にブザは鳴動し無くなります。

コマンドモード		書　式	PC モード		書　式
ブザコマンド設定	コマンド	BS[CR]	ブザコマンド設定	コマンド	BS
	レスポンス	OK[CR]		レスポンス	OK[CR][LF]

BR：ブザコマンド解除

ブザ鳴動コマンドを無効にします。タグアクセス成功時にブザは 0.1 秒鳴動します。

コマンドモード		書　式	PC モード		書　式
ブザコマンド解除	コマンド	BR[CR]	ブザコマンド解除	コマンド	BR
	レスポンス	OK[CR]		レスポンス	OK[CR][LF]

B：ブザ鳴動コマンド

リーダ／ライタに実装されたブザの鳴動を制御します。ブザの短発振、長発振、3 倍長発振、及び、発振停止（それらを「発振パターン」と総称します）を、パラメータで指定することが出来ます。

※ ブザコマンド解除時には、本コマンドは「コマンドエラー」となります。

※ 本コマンドは、最大 128 文字の発振パターンを登録出来ますが、このパターンの実行が終了する迄（最大約 40 秒）、他のコマンドを実行できません。

コマンドモード		書　式
ブザ鳴動コマンド	コマンド	B<bzz<[CR] （bzz：ブザ発振パターン[0,1,2,3] 最小 1 文字、最大 128 文字 0 = 0.1 秒の発振停止 1 = 0.1 秒の発振 2 = 0.2 秒の発振 3 = 0.3 秒の発振 ）
		bzz は数字の羅列になる為、末尾の“<”及び[CR]によってパラメータの終了を表わします(末尾の“<”は省略出来ます)。
	レスポンス	OK[CR] （発振動作終了後に応答します）
	制約	ブザの発振パターンは最大 128 文字登録できます。
PC モード		書　式
ブザ鳴動コマンド	コマンド	B<bzz< （bzz：ブザ発振パターン[0,1,2,3] 最小 1 文字、最大 128 文字 0 = 0.1 秒の発振停止 1 = 0.1 秒の発振 2 = 0.2 秒の発振 3 = 0.3 秒の発振 ）
		bzz は数字の羅列になる為、末尾の“<”によってパラメータの終了を表わします。
	レスポンス	OK[CR][LF]（発振動作終了後に応答します）
	制約	ブザの発振パターンは最大 128 文字登録できます。

ブザの鳴動は、■を 0.1 秒の鳴動、□を 0.1 秒の無音状態として表現します。

下記例は、何れも、コマンドモード時は①末尾のカンマは省略できます ②[CR]を付加して下さい。

例 1)0.4 秒間の鳴動させるには

B<22<　　または、

B<13<　　または、

B<31<　　と入力します。

■■■■　　(0.4 秒間の鳴動)

（お気付きの様に、B<112< B<121< B<211< B<1111< の 4 パターン何れも上記と同じ鳴動をします）

例 2)0.1 秒間の鳴動を 0.1 秒間隔で 4 回行うには、

B<1010101<　　**と入力します。**

■□■□■□■　(0.1 秒間の鳴動を 0.1 秒間隔で 4 回)

３－２．ISO14443 コマンド

XX：スキャン

応答範囲内にある ISO14443 をスキャンし、検知した UID を応答します。

コマンドモード		書　式	
スキャン	コマンド	XX[CR]	
	レスポンス	検知された時 ID[CR]	検知されなかった時 None[CR]
		ID：検知された ISO14443 の UID(16 進数 5 or 7By)	
	制約	複数のカードを一度に検知することは出来ません。	
PC モード		書　式	
スキャン	コマンド	XX	
	レスポンス	検知された時 ID[CR][LF]	検知されなかった時 None[CR][LF]
		ID：検知された ISO14443 の UID(16 進数 5 or 7By)	
	制約	複数のカードを一度に検知することは出来ません。	

表示例（UID 4By の ISO14443 の場合）

```
B2BC0DCBC8
```

表示例（UID 7By の ISO14443 の場合）

```
9909BB66300000
```

※ 検知された ISO14443 が UID 4By のものならば､チェックバイトを伴った 5By の UID を応答します。
※ 検知された ISO14443 が UID 7By のものならば、チェックバイトを伴わず、7By の UID を応答します。

XS：連続スキャン開始

応答範囲内にある ISO14443 を検知するまでスキャンを続けます。

コマンドコードが異なるりますが、前項の「XX:スキャン」と発行例も成功時応答例も同様なので、詳述は省略します。

但し、本コマンドは ISO14443 を検知するまで連続してスキャンを実行しますので、連続スキャンを終了するには、上位側より何らかの文字を送信して下さい。

リーダ／ライタは”None” と応答し、連続スキャンを終了します。

RU：UL 系タグ 全件読出

応答範囲内にある UL 系タグ内の全データを読出します。
一度に読出せるカードは 1 枚です。

<table>
<tr><th colspan="2">コマンドモード</th><th colspan="2">書　式</th></tr>
<tr><td rowspan="4">UL 系タグ
読出</td><td>コマンド</td><td colspan="2">RU[CR]</td></tr>
<tr><td rowspan="3">レスポンス</td><td>成功時
DATA［CR］</td><td rowspan="3">DATA：
タグ内のデータを第 00 ブロックより応答します。
カンマ等のブロック間の区切りは無しにデータを連続して応答します。</td></tr>
<tr><td>失敗時(全く読出せない場合)
［エラーコード][CR]</td></tr>
<tr><td>失敗時(途中まで読出せた場合)
DATA［CR］
※エラーコードは応答されません。。</td></tr>
<tr><td>制約</td><td colspan="2">複数のカードを一度に読むことは出来ません。</td></tr>
<tr><th colspan="2">PC モード</th><th colspan="2">書　式</th></tr>
<tr><td rowspan="4">UL 系タグ
読出</td><td>コマンド</td><td colspan="2">RU</td></tr>
<tr><td rowspan="3">レスポンス</td><td>成功時
DATA［CR][LF]
(DATA［CR][LF]…
DATA［CR][LF])</td><td rowspan="3">DATA：
タグ内のデータを第 00 ブロックより 4 ブロック(16By)毎に改行して応答します。</td></tr>
<tr><td>失敗時(全く読出せない場合)
［エラーコード][CR][LF]</td></tr>
<tr><td>失敗時(途中まで読出せた場合)
DATA［CR][LF]
(DATA［CR][LF]…
DATA［CR][LF])
※エラーコードは応答されません。</td></tr>
<tr><td></td><td>制約</td><td colspan="2">複数のカードを一度に読むことは出来ません。</td></tr>
</table>

◎ その他の制約

UL 系タグは、読出コマンドで指定したブロックより 4 ブロック・計 16By のデータを読出します。4 ブロック読出す前に最終ブロックに到達した場合は 00 ブロックより読出し、計 16By を応答します。

本コマンドは、第 00 ブロックより 4 ブロック単位の読出を継続して行ないますが、上記の性質を利用し、初めに読出した第 00 ブロックと同じ内容のブロックを読出した時には「第 00 ブロックに戻った」ものとしてその前のブロックまでを応答して終了します。

また、連続読出の途中で「読出エラー」が発生した時は「最終ブロックに到達したもの」としてエラーレスポンスを応答しません。

従って、第 00 ブロックと同じ内容を書込まれたブロックがあった場合、本コマンドではそれ以降のブロックは読出されません。また、読出途中で「タグがアンテナ応答範囲を外れた」等で読出に失敗した場合「タグの終端を超えた為失敗したもの」と解釈し、エラーレスポンスは応答されません。

例）Mifare Ultralight 内の全データを読出します。
RU　　と入力します（コマンドモードの時は[CR]を追加して下さい）。
読出が成功した場合、タグ内の全データ 64By が応答されます。（表示例は省略します）

※ DNA の様にコマンドの異なるものや、セキュリティの掛かったブロックは読出せません。

t+, t-：スルーモード開始／終了 コマンド

スルーコマンドは、リーダ/ライタ･タグ間のエアインターフェイスコマンドの内容を上位から直接発行し、タグよりの応答を上位に直接応答する為のものです。

発行するエアインターフェイスコマンドは目的とする動作により様々ですが、通常複数の送受信を行いますので、一連のスルーコマンドが終了するまでの間「RF 発振」を継続させる必要が有ります。その設定が、スルーモードです。

後述の、NA,NW 等の組込コマンドは、発行されたコマンド及びパラメータに従ってタグに対しエアインターフェイスコマンドを発行し、タグのレスポンスより成否及び継続を判断し実行しており、その一連の動作は「RF 波発振」状態で実行されます。

リーダ/ライタは「スルーモード終了」状態で起動します。スルーモードは、「スルーモード開始」コマンドの他に、後述の「スルーコマンド」発行によってもモードが開始されます。

ISO14443 専用機以外のリーダ/ライタでは、他のタグ種に設定するとスルーモードは停止します。

コマンドモード		書　式	PC モード		書　式
スルーモード開始	コマンド	t+[CR]	スルーモード開始	コマンド	t+
	レスポンス	+OK[CR]		レスポンス	+OK[CR][LF]
スルーモード終了	コマンド	t-[CR]	スルーモード終了	コマンド	t+
	レスポンス	-OK[CR]		レスポンス	-OK[CR][LF]

t：スルーコマンド

上位側より発行した文字列を直接エアインターフェイスでカードに送出し、カードよりの応答(同じくエアインターフェイス)を上位に応答します。

コマンドモード		書　式
スルーコマンド	コマンド	t<Data[CR]
		Data:エアインターフェイスで送出するコマンド(16 進数:198By 迄)
	レスポンス	nn<Rsp[CR]
		nn ：Rsp の By 数。Rsp なしは nn=00 Rsp:タグからのエアインターフェイス応答(16 進数)
	制約	Data,Rsp 共最大 198By です。超過の場合、Data は発行時にエラーとなり、Rsp は 198By のみ応答します。 ※ DNA の Rsp は 198By を上回ることは有りません。
PC モード		書　式
スルーコマンド	コマンド	t<Data,
		Data:エアインターフェイスで送出するコマンド(16 進数:198By 迄) ※末尾のカンマは入力終了を示します
	レスポンス	nn,Rsp[CR][LF]
		nn ：Rsp の By 数。Rsp なしは nn=00 Rsp:タグからのエアインターフェイス応答(16 進数)
	制約	Data,Rsp 共最大 198By です。超過の場合、Data は発行時にエラーとなり、Rsp は 198By のみ応答します。 ※ DNA の Rsp は 198By を上回ることは有りません。

※ Rsp が 8bt 単位で無い場合、半端の bt 数を追加出力します。

例)Ack 応答の場合　　4-01,0A[CR]　(ACK は 1010b の 4bit で応答されます)

リーダ/ライタは、文字列(16 進数)の末尾のデリミタ(コマンドモードは[CR]、PC モードは"<")を受信すると、それまでの文字列をバイナリでカードに送信します。

一定時間以内に応答が無い場合は、00[CR]を応答します。

※ 下記表の例に示した「ISO14443-4 プロトコル活性化」に成功すると、DNA はスキャンコマンドに応答しなくなります。後述の「DA:DNA の Key 認証」コマンドでは、成功時にこの状態になり RF 発振が継続されます。
一連の動作をスキャンより再開したい場合は、一度スルーモードを終了させるか、タグをアンテナ応答範囲より離してから実行して下さい。

例)NKL を除く「DNA 専用コマンド」では、コマンド発行直後に以下と同様の動作を行っています。

コマンド	レスポンス	内容	備考
t-	-OK	スルーモード終了	R/W がスルーモード中の場合、DNA はスキャンコマンドを受け付けないので、安全の為モードを終了させる
t+	+OK	スルーモード開始	
XX	UID	スキャン(通常コマンド)	RF 制御 IC を ISO14443 に設定する
t<E080	06<067777710280	RATS 送信、ATS 受信	NTag424DNA を示す ATS を応答
t<001100	01<D0	PPS 発行	通信 By 数等を設定

※ これらは DNA の ISO14443-4 プロトコルを活性化する動作です。
※ これらの動作を含む組込コマンドでは、RATS に対し DNA の ATS が王乙されなければ ER00(タグなし)のエラーを応答します。
※ 詳しくお知りになりたい場合は ISO14443 の文書を、DNA の操作をスルーコマンドで行う場合には DNA のデータシートを参照下さい。

３－３．DNA 専用コマンド

パラメータの Key について

- DNA には、Key00～04 の 5 種類に Key が有り、いずれも 16By の 16 進数です。
  Key00 はマスターKey です。

- R/W は､EEP メモリに 16By の Key 値を 16 種類(Key 番号:00～0F)記憶させることが出来ます(この値は電源が Off されても記憶されます)。
  DNA の Key のデフォルト値は 5 種共全 00h です｡この全 00h の Key は一番使用頻度が高いので、上記の 16 種類とは別に、Key 番号 FF を指定すると全 00h が用いられます(Key 番号 FF の Key 値は変更出来ません)。

- DNA 及び R/W には Key と称するものが複数あるので、名称を統一します。
  DNA のカードには 3 つのファイルが有り、R/W はその内 NDEF ファイルと CC ファイルにアクセスします。それらのファイルには Key00～04 の 5 種類の Key が対応しており、R/W にはそれらを認証する Key の値を 00～0F の 16 種類 R/W に登録(ロード)することが出来ます。
  本書に於いて、DNA の Key を DNA Key、R/W にロードする Key を認証 Key と称します。
  また、後述する Key バージョンも 2 桁となるので、5 種の DNA Key は 0～4 の 1 桁で扱います。

- 前項の Key 表現の用法は、①DNA Key 0 を認証 Key0E で認証して NDEF を書込む、②DNA Key2 の値を認証 KeyFF から 02 に書換える、等です。

NKL：認証 Key のロード

NTag424DNA の認証等に使用する 16By の Key を R/W の EEP ロムに登録します。

コマンドモード		書　式	
認証 Key のロード	コマンド	NKL<kn<Data[CR] kn　：R/W にロードする認証 Key(00～0F) Data: ロードする認証 Key の値（16 進数 16By）	
	レスポンス	成功時　　OK[CR]	失敗時　　エラーコード
PC モード		書　式	
認証 Key のロード	コマンド	NKL<kn<Data kn　：R/W にロードする認証 Key(00～0F) Data: ロードする認証 Key の値（16 進数 16By）	
	レスポンス	成功時　　OK[CR][LF]	失敗時　　エラーコード

※ 認証 Key は 00～0F の 16 種類登録出来ます。
※ 認証 Key を FF に指定すると全 00h の値が使用されます。全 00h を登録する必要は有りません。

NKW：DNA の認証 Key 書換

コマンドモード		書　式	
DNA Key の書換	コマンド	NKW<k<ko<kn(<k0)<kv[CR] k　:認証する DNA Key 0～4 ko ： 上記 k の変更前の認証 Key(00～0F 及び FF) kn ： 上記 k の変更前の認証 Key(00～0F 及び FF) k0 ： DNA Key0 に登録されている値の認証 Key(00～0F 及び FF) ※ 上記 k が 0(マスターKey の書換)の場合、k0 は入力不要です。 kv ： キーバージョン(00～FF の任意の値)	
	レスポンス	成功時　OK[CR]	失敗時　エラーコード
PC モード		書　式	
DNA Key の書換	コマンド	NKW<k<ko<kn(<k0)<kv k　:認証する DNA Key 0～4 ko ： 上記 k の変更前の認証 Key(00～0F 及び FF) kn ： 上記 k の変更前の認証 Key(00～0F 及び FF) k0 ： DNA Key0 に登録されている値の認証 Key(00～0F 及び FF) ※ 上記 k が 0(マスターKey の書換)の場合、k0 は入力不要です。 kv ： キーバージョン(00～FF の任意の値)	
	レスポンス	成功時　OK[CR][LF]	失敗時　エラーコード

※ 上表 ko kn は old と new の o,n で、k0 は DNA Key0 を表します。
※ 使用する認証 Key(ko､kn,k0)の値は、予め前述の「NKL コマンド」で登録しておいて下さい。

例)DNA Key0 の値を、カード発行時初期値より認証 Key00 に変更する場合
　キーバージョン(任意)は 01 とします。
　NKW<0<FF<00<01[CR]

例)Key01 の値を、カード発行時初期値より 02 にロードされた値に変更する場合
DNA Key0 は認証 Key01 が登録されているものとし、キーバージョン(任意)は 05 とします。
　NKW<1<FF<02<01<05 [CR]

NA：DNA の Key 認証

認証後に、組込まれていないコマンドをスルーコマンドで発行することを想定して組込みました。
現在登録されている DNA Key が認証 Key と一致しているか、の確認にも使用出来ます。

コマンドモード		書　式	
DNA の認証	コマンド	NA<k<kn [CR] k　:認証する DNA Key 0～4 kn　: 上記 k の認証 Key(00～0F 及び FF)	
	レスポンス	成功時　　欄外を参照下さい	失敗時　　エラーコード
PC モード		書　式	
DNA の認証	コマンド	NW<k<ko<kn(<k0)<kv k　:認証する DNA Key 0～4 kn　: 上記 k の認証 Key(00～0F 及び FF)	
	レスポンス	成功時　　欄外を参照下さい	失敗時　　エラーコード

- 失敗時には、認証エラーの ER01 が応答されます。
- 成功時には、TI(4By) < K_Mac(16By) < K_Enc(16By) が応答され、スルーモードが継続されます(TI:トランザクション ID、K_Mac,K_Enc:以降の計算に用いるエンコードや MAC 生成 Key)。
- 応答された値を用いて外部で AES 計算等を行い、t コマンドで DNA にアクセスコマンドを発行することが出来ます。

※ t コマンド以外の「DNA 専用コマンド」を発行した際に、コマンド成功やコマンドエラー(ER04)以外のエラーとなった場合は、スルーモードが終了します。

NW：NDEF の書込と設定

URL をセキュリティ付の NDEF として DNA への書込と設定を行います。

コマンドモード		書　式	
NDEF 書込	コマンド	NW<k<kn<URL<mir<mac[CR] k　：認証する DNA Key(0～4 の 1 桁) kn　：上記 k の認証に用いる、認証 Key(00～0F,FF) URL ：NDEF として書込む URL mir ：「ミラー」を応答する位置を示す文字列 mac ：「CMAC」を応答する位置を示す文字列	
	レスポンス	成功時　　OK[CR]	失敗時　　エラーコード
	制約	URL の文字数は、IDcode で省略できるものを除き 168 文字迄です。 mir 及び mac に登録できる文字数は各々8 文字までです。 mir 及び mac は「URL 内の位置を限定」出来る文字列にして下さい。	
PC モード		書　式	
NDEF 書込	コマンド	NW<k<kn<URL<mir<mac k　：認証する DNA Key(0～4 の 1 桁) kn　：上記 k の認証に用いる、認証 Key(00～0F,FF) URL ：NDEF として書込む URL mir ：「ミラー」を応答する位置を示す文字列 mac ：「CMAC」を応答する位置を示す文字列	
	レスポンス	成功時　　OK[CR][LF]	失敗時　　エラーコード
	制約	URL の文字数は、IDcode で省略できるものを除き 168 文字迄です。 mir 及び mac に登録できる文字数は各々8 文字までです。 mir 及び mac は「URL 内の位置を限定」出来る文字列にして下さい。	

本コマンドを実行すると、後述の「4.応答の複合化と照合」に記した「UID ミラーの複合化」及び「MACt(CMAC)の照合」に用いる DNA の Key も設定されます。

※ 現在は、NXP:タグメーカの資料に準じ、固定で、前者を DNA Key2、後者を DNA Key1 としています。

現在のファームでは、「ミラー」と「CMAC」、①URL に「ミラー」「CMAC」が共に有ること、②位置は「ミラー」が先、にしか対応出来ていません。また、③「ミラー」の応答が表中“cmac”の文字列を上書きする検査、④「CMAC」が URL の末尾を上回る検査、も含まれておりません。

※ 今後の改良点と考えております。

以下の(存在しない)URL を例とします。

http://sample-url.com/?mirror=00000000000000000000000000000000&cmac=0000000000000000

NW コマンドは以下になります(DNA Key=0、認証 Key=FF とします)。

NW<0<FF<http://sample-url.com/?mirror=00000000000000000000000000000000
&cmac=0000000000000000<?mirror=<&cmac=[CR]

mirror=に続く 32 桁の 0 の位置に「ミラー」を、cmac=に続く 16 桁の 0 の位置に「CMAC」を応答させるには、表中の mir を“mirror=”、表中の mac を“cmac=”とします。

上記 URL の例では、mir を“r=”、mac を“c=”とすることも出来ますが、各々、URL 内に「1 か所しか無い」文字列を指定して下さい。

※ mir,mac に続く 2 ヶ所の「0 の連続」は「ミラー」「CMAC」が応答されるときに上書きされます。0 の連続である必要はありませんが、誤登録を防ぐ為「見易い」「確認し易い」文字にして下さい。

※ 初期状態の DNA は NDEF ファイルのアクセス権(認証する DNA Key)が変更されます。末尾の資料に説明を記しています。

NRP：NDEF 読出(平文)

P はプレーン(平文)を表します。

コマンドモード		書　式	
書込	コマンド	NRP[CR]	
	レスポンス	成功時　　OK[CR]	失敗時　　エラーコード
PC モード		書　式	
書込	コマンド	NRP	
	レスポンス	成功時　　OK[CR][LF]	失敗時　　エラーコード

※ UID ミラーは、C7h(1By),UID(7By),カウンタ(3By)+ダミー(5By)の 16 進数 16By が ASCII 展開で応答されます。

NRP [CR]

パラメータは有りません。NTag424DNA に書込まれた NDEF を URL の形式で応答します。

セキュリティ付の NDEF の場合、URL ミラー(16By)及び照合用 CMAC(8By)が暗号化されたまま応答されます。復号化については次章に記します。

前述の NW コマンドで書込んだ URL を読み出した場合、以下の様に応答されます。

http://sample-url.com/?mirror=D0013F66CEFA9B7961C357A59878D1D9&cmac=88EBA511E54C251E

NRD：NDEF 読出(複合化)

前述の NRP コマンドでは暗号化された UID ミラーを複合化して応答します。

照合用 CMAC も計算して照合し、一致すればそのまま、不一致ならば末尾に<ER01 が応答されます。

コマンドモード		書　式	
書込	コマンド	NRD<km<kc<mir<mac[CR] km　：「ミラー」を複合化する Key の番号 kc　：「CMAC」を照合する Key の番号 mir：「ミラー」が応答される位置を示す文字列(NW コマンドを参照下さい) mac：「CMAC」が応答される位置を示す文字列(NW コマンドを参照下さい)	
	レスポンス	成功時　　欄外を参照下さい。	失敗時　　エラーコード
PC モード		書　式	
書込	コマンド	NRD<km<kc<mir<mac km　：「ミラー」を複合化する Key の番号 kc　：「CMAC」を照合する Key の番号 mir：「ミラー」が応答される位置を示す文字列(NW コマンドを参照下さい) mac：「CMAC」が応答される位置を示す文字列(NW コマンドを参照下さい)	
	レスポンス	成功時　　欄外を参照下さい。	失敗時　　エラーコード

前項「NRP:NDEF 読出(平文)」に示された URL を本コマンドで読出すと以下の様になります。

この例の、km の値は全 22h、kc の値は全 11h です。

http://sample-url.com/?mirror= C704885E921B70808700001E43B95D22&cmac=88EBA511E54C251E

「ミラー」は復号化して応答されます。CMAC の称号が不一致の場合、末尾に<ER01 が付加されます。

「ミラー」C704885E921B70808700001E43B95D22 の内容は以下の通りです。

C7	: UID とカウンタがミラー応答され、UID が 7By であることを示す。
04885E921B7080	: UID
870000	: カウンタ。000087h=135 を意味します。
1E43B95D22	: ダミーデータ

NC：CC ファイル設定

DNA に含まれる CC(Capability Container)ファイルに「書込禁止」を登録します。
この「書込禁止」は NFC リーダ/ライタが DNA アクセス時に「NDEF が書込禁止」であることを認識するためのものですが、この動作を行っても前述の「NW:NDEF の書込と設定」を行うことが出来ます。
実際に DNA の NDEF を変更出来ない様にするには、次項のコマンドを実行して下さい。

コマンドモード		書　式	
書込	コマンド	NC＜k<kn[CR] k　：CC ファイルの DNA Key kn　：CC ファイルの認証 Key 番号	
	レスポンス	成功時　　OK[CR]	失敗時　　エラーコード
PC モード		書　式	
書込	コマンド	NC＜k<kn k　：CC ファイルの DNA Key kn　：CC ファイルの認証 Key 番号	
	レスポンス	成功時　　OK[CR][LF]	失敗時　　エラーコード

※ 本コマンドは、通常 00h(書込可)が登録されている CC ファイルの書込アクセスコンディションに FFh(書込禁止)を書込みます。異なる値を登録することは出来ません。

NL：DNA のアクセス権変更

DNA の NDEF ファイル 又は CC ファイルの、書込アクセス権を変更します。
現在のアクセス権を確認することも出来ます。

コマンドモード		書　式	
書込	コマンド	NL＜k<kn<file<ar[CR] k　：file の(変更前の)DNA Key kn　：file の認証 Key 番号 file: C(CC ファイル) 又は N(NDEF ファイル) ar　：アクセス権。　アクセス権変更時:0～4,F ， 現設定の確認時: “?” **※ ar を F にすると、書込/変更が禁止になります。**	
	レスポンス	変更成功時　OK[CR] 確認時　　xxEx[CR]　　x:DNA Key	失敗時　　エラーコード
PC モード		書　式	
書込	コマンド	NL＜k<kn<file<ar k　：file の(変更前の)DNA Key kn　：file の認証 Key 番号 file: C(CC ファイル) 又は N(NDEF ファイル) ar　：アクセス権。　アクセス権変更時:0～4,F ， 現設定の確認時: “?” **※ ar を F にすると、書込/変更が禁止になります。**	
	レスポンス	変更成功時　OK[CR] 確認時　　xxEx[CR][LF] x:DNA Key	失敗時　　エラーコード

※ 上表の ar を “?” とすると、現在のアクセス権が表示されます。
※ アクセス権については、末尾の資料を参照下さい。

４．応答の複合化と照合

DNA をスマートフォン等にタッチした場合、「3-3.DNA 専用コマンド」の「NRP:NDEF 読出(平文)」で読出された URL がサーバーに送信されます。
この URL には、「ミラー」及び「CMAC」が含まれています。
サーバー側では、応答された暗号化データを以下の方法で復号化･照合することが出来ます。
尚、前述の「NRD:NDEF 読出(複合化)」では下記と同様の動作を行っています(同コマンドの説明を参照下さい)。

４―１．「ミラー」の複合化

UID ミラー16By は、複合 Key(16By)を用いて AES デコードすると、以下が算出されます。
復号 Key は DNA のマスターKey(DNA Key0)とは異なる Key を用います。復号された「ミラー」は以下の形式となります。

[“C7”+ UID + カウンタ + ダミー5By]

“C”	UID とカウンタがミラーで応答されることを示します。
“7”	UID が 7By であることを示しています。
UID	DNA の UID。
カウンタ	3By の 16 進数で下位から応答されます。 例)258 の場合 02 01 00、65539 の場合 03 00 01 となります。
ダミー	ミラーを 16By で応答する為に DNA が付加した乱数で、内容に意味は有りませんが、読出す都度異なる値が応答されるので、暗号化がより複雑(暗号解読が難)になります。

４－２．「CMAC」の照合

以下の計算で、応答された MACt が正しいか否かを確認することが出来ます。但し、計算に用いられる検証 Key はマスターKey とも上記の複合 Key とも異なる DNA Key を用います。
照合計算は、下記の様に、定数と上記で得られた UID･カウンタ値を用います。

1. Key=【検証 Key】、Data=【“3CC300010080”+上記 UID+上記カウンタ】、IV=【全 00h】、で、CMAC(16By)を算出します。
2. 1.の算出結果を Key とし、Data=【空(Empty)データ】、IV=【全 00h】で、CMAC を算出します。
3. 算出された CMAC(16By)の MACt(8By)が読出された値と一致するかを確認して下さい。
   MACt は 0 起算として CMAC の奇数バイトを抽出したものです。

５　資料

５－１．URL ID Code

URL を NDEF 形式で登録する際に、冒頭の「定型句」をコードで省略して登録することが出来ます。
省略出来る「冒頭の文字列」は右表の「Text」の文字列です。
URL の冒頭が「Code」の 01～23(16 進数:全 35 種類)の「Text」に当てはまるものがない場合は、何も省略されません。

Code	Text
00	なし
01	http://www.
02	https://www.
03	http://
04	https://
05	tel:
06	mailto:
07	ftp://anonymous:anonymous@
08	ftp://ftp.
09	ftps://
0A	sftp://
0B	smb://
0C	nfs://
0D	ftp://
0E	dav://
0F	news:
10	telnet://
11	imap:
12	rtsp://
13	urn:
14	pop:
15	sip:
16	sips:
17	tftp:
18	btspp://
19	btl2cap://
1A	btgoep://
1B	tcpobex://
1C	irdaobex://
1D	file://
1E	urn:epc:id:
1F	urn:epc:tag:
20	urn:epc:pat:
21	urn:epc:raw:
22	urn:epc:
23	urn:nfc:

５－２．アクセス権について

DNA の初期状態のアクセス権は、以下の様になっています。

ファイル	アクセス権
NDEF ファイル	Ｅ０Ｅ Ｅ
CC.ファイル	００Ｅ０

表内のアクセス権は、前より ReadWrite,Change,Read,Write に対応しています。その値は下表のとおりです。

アクセス権	内　　容
0～4	アクセスに使用できる DNA Key
E	どの DNA Key でもアクセス可
F	アクセス不可

前述の「NW:NDEF の書込と設定」コマンドでは、NDEF ファイルのアクセス権を、認証に使用した DNA Key を x とし、
xxEx に書換えます。
初期状態の DNA では、0～4 の DNA Key は全て全 00h なので、認証 Key=FF を指定すると認証出来ます。
初期状態の DNA に対して NW コマンドを実行すると、コマンド成功後のアクセス権は、
NW<0<FF<…の場合、00E0 となり、NW<1<FF<…の場合は 11E1 となります。同様に 2～4 も順に 22E2,33E3,44E4 が設定されます。

※ NW コマンド成功後、NDEF ファイルへの読出を除くアクセスは、NW コマンドで用いた DNA Key を用いて下さい。
※ セキュリティ向上の為、NKW コマンドで DNA Key の値を変更することをお勧めします。
※ このアクセス権を変更するには「NL:DNA のアクセス権変更」を行って下さい。

６　品質保証及び保証書

６－１　保証期間

納入しました商品の保証期間は、ご指定場所に納入後1 年間と致します。

６－２　保証範囲

正常なご使用状態のもとで保証期間内に万一故障した場合、その商品の故障部品の交換または修理を無償で行わせて頂きます。

ただし、次に該当する場合は、この補償の対象範囲から除外させていただきます。

（イ）　ご使用上の誤り、および不当な修理や改造による故障または損傷。
（ロ）　お買い上げ後の取付場所の移動、落下、引っ越し、輸送などによる故障または損傷。
（ハ）　火災、地震、風水害、落雷、その他の天災、地変、公害、塩害、ガス害、異常電圧や指定外電源使用等により生じた故障または損傷。
（ニ）　接続している他の機器、その他の外部要因に起因して生じた故障または損傷。
（ホ）　取扱説明書に記載されている使用条件以外で使用した場合の故障または損傷。
（ヘ）　消耗品の交換、仕様変更など。

６－３　サービスの範囲

上記の保証につきましては日本国内においてのみ有効です。

販売日付及び販売店印のない保証書は無効です。

- 保証期間経過後の修理につきましては、有償にて御承りますので、お買い上げの販売店へご相談下さい。

＜免責事項＞

1. お客様がご購入された製品について、弊社に故意または重大な過失があった場合を除き、債務不履行または不法行為に基づく損害賠償責任は、当該製品の購入代金を限度と致します。
2. お客様がご購入された製品について、隠れた瑕疵があった場合は、この保証書の規定にかかわらず、無償にて当瑕疵を修理し、または、瑕疵のない製品または同等品に交換致しますが、当該瑕疵に基づく損害賠償の責に任じません。
3. 弊社における保証は、お客様がご購入された製品の機能に関するものであり、非接触ＩＣカード・タグ等に記録されたデータ の消失または破損について保証するものではありません。

販売店印

改訂歴

2025/01/10　第 1 版 発行

改　訂	改　訂　箇　所	改　訂　理　由