集積回路

データシート

mifare
標準カード IC
MF1 IC S50
機能仕様

製品仕様

改訂 5.1

May 2001

Philips Semiconductors

PHILIPS

目次

1 特徴

1．1 MIFARE RF ｲﾝﾀｰﾌｪｰｽ (ISO/IEC 14443 A)

- ﾃﾞｰﾀと電源ｴﾈﾙｷﾞの非接触通信 (ﾊﾞｯﾃﾘｰは必要無し)
- 動作間隔： 100mm (ｱﾝﾃﾅ方位による)
- 動作周波数：13.56 MHz
- 高速度転送：106kbi/s
- ﾃﾞｰﾀの高整合性：16 Bit CRC, ﾊﾟﾘﾃｨ, bit coding, bit counting
- 完全な非衝突
- 発券標準処理時間：< 100ms (ﾊﾞｯｸｱｯﾌﾟ管理含む)

1．2 EEPROM

- 1Kﾊﾞｲﾄ, 16 ｾｸﾀ, 4 ﾌﾞﾛｯｸ/ｾｸﾀ, 16 ﾊﾞｲﾄ/ﾌﾞﾛｯｸ
- 各ﾒﾓﾘﾌﾞﾛｯｸに対してﾕｰｻﾞ定義可能なｱｸｾｽ条件設定
- 10年間ﾃﾞｰﾀ保持
- 100,000回のﾃﾞｰﾀ書込み

1．3 ｾｷｭﾘﾃｨ

- 共有3ﾊﾟｽ認証 (ISO/IEC DIS9798-2)
- 反射攻撃から保護されたRF-ﾁｬﾈﾙ上のﾃﾞｰﾀ暗号化
- ｾｸﾀｰ当たり二つの個別ｷｰでｷｰ階層によるﾏﾙﾁｱﾌﾟﾘｹｰｼｮﾝをｻﾎﾟｰﾄ (ｱﾌﾟﾘｹｰｼｮﾝ毎)
- 各ｶｰﾄﾞ毎にﾕﾆｰｸなｼﾘｱﾙ番号
- 転送ｷｰは、ﾁｯﾌﾟ提供時にEEPROMへのｱｸｾｽを保護

2 概説

MIFARE MF1 IC S50はISO/IEC 14443A準拠の非接触型ｽﾏｰﾄｶｰﾄﾞです。通信層(MIFARE RF ｲﾝﾀｰﾌｪｰｽ)はISO/IEC 14443A標準のﾊﾟｰﾄ2/3に準拠しています。ｾｷｭﾘﾃｨ層はMIFARE Classic famillyの安全なﾃﾞｰﾀ交換の分野で立証済みの「CRYPTO1」ｽﾄﾘｰﾑ暗号を使用しています。

2．1 非接触型電源ｴﾈﾙｷﾞとﾃﾞｰﾀ転送

MIFAREｼｽﾃﾑに於いて、MF1 IC S50 は2～3回巻のｺｲﾙに接続されていて電源を持たない非接触型ｽﾏｰﾄｶｰﾄﾞ型ﾌﾟﾗｽﾃｨｯｸに収納されています。ﾊﾞｯﾃﾘｰは必要ありません。ｶｰﾄﾞがﾘｰﾄﾞﾗｲﾄ機器(RWD)の近傍に置かれると、高速RF通信ｲﾝﾀｰﾌｪｰｽにより106KBits/sでﾃﾞｰﾀ通信が可能になります

2．2 非衝突

高性能な非衝突型の機能により同時に複数のｶｰﾄﾞを動作させる事が可能です。非衝突型ｱﾙｺﾞﾘｽﾞﾑはｶｰﾄﾞを個々に選択し、選択されたｶｰﾄﾞとの処理が他のｶｰﾄﾞとの影響によりﾃﾞｰﾀが破損する事はなく適切に行われる事を保証します

2．3 有益性

MIFARE ｼｽﾃﾑはﾕｰｻﾞにとって最適な有益性をもたらすように設計されています。例えば高速ﾃﾞｰﾀ転送速度により完全な発券処理が100ms以下で制御される事が可能になっています。このようにMIFAREｶｰﾄﾞはｹﾞｰﾄでの膨大な処理量が発生するRWDｱﾝﾃﾅ部で留まる事はなくﾊﾞｽ上の搭乗回数を減少させます。MIFAREｶｰﾄﾞは財布の中でも、その財布の中にｺｲﾝがあっても読み取りできます

2．4 ｾｷｭﾘﾃｨ

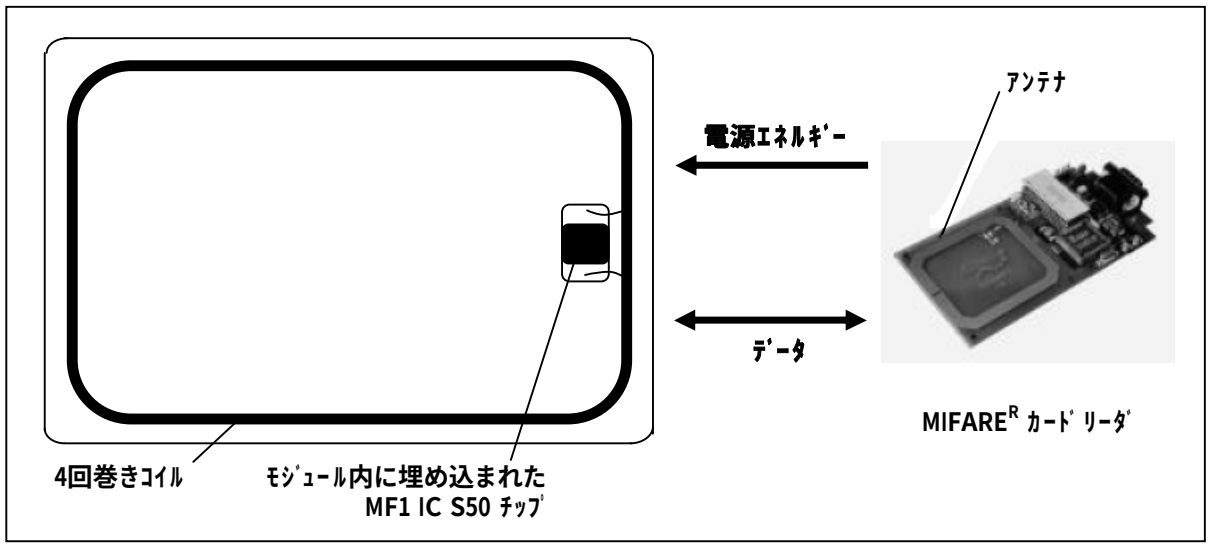
不正に対して特別な重点対策がｾｷｭﾘﾃｨ上施されました。相互ﾁｬﾚﾝｼﾞｺｰﾄﾞ、応答認証、ﾃﾞｰﾀ暗号、および通報認証ﾁｪｯｸはどんな種類の改ざんからもｼｽﾃﾑを保護し発券ｱﾌﾟﾘｹｰｼｮﾝを際立たせます。変更不可のｼﾘｱﾙ番号は各ｶｰﾄﾞの唯一性を保証します

2．5 ﾏﾙﾁ ｱﾌﾟﾘｹｰｼｮﾝ機能

MIFAREｼｽﾃﾑはﾌﾟﾛｾｯｻｰｶｰﾄﾞの特徴に匹敵する真のﾏﾙﾁｱﾌﾟﾘｹｰｼｮﾝ機能を提供します。各ｾｸﾀｰの二つの異なるｷｰはｷｰ階層構造によりｼｽﾃﾑをｻﾎﾟｰﾄします

2．6 出荷ｵﾌﾟｼｮﾝ

- 製造素材(ｳｪﾌｧｰ)の金型
- 製造素材(ｳｪﾌｧｰ)の(Bumped)金型
- ﾁｯﾌﾟｶｰﾄﾞﾓｼﾞｭｰﾙ

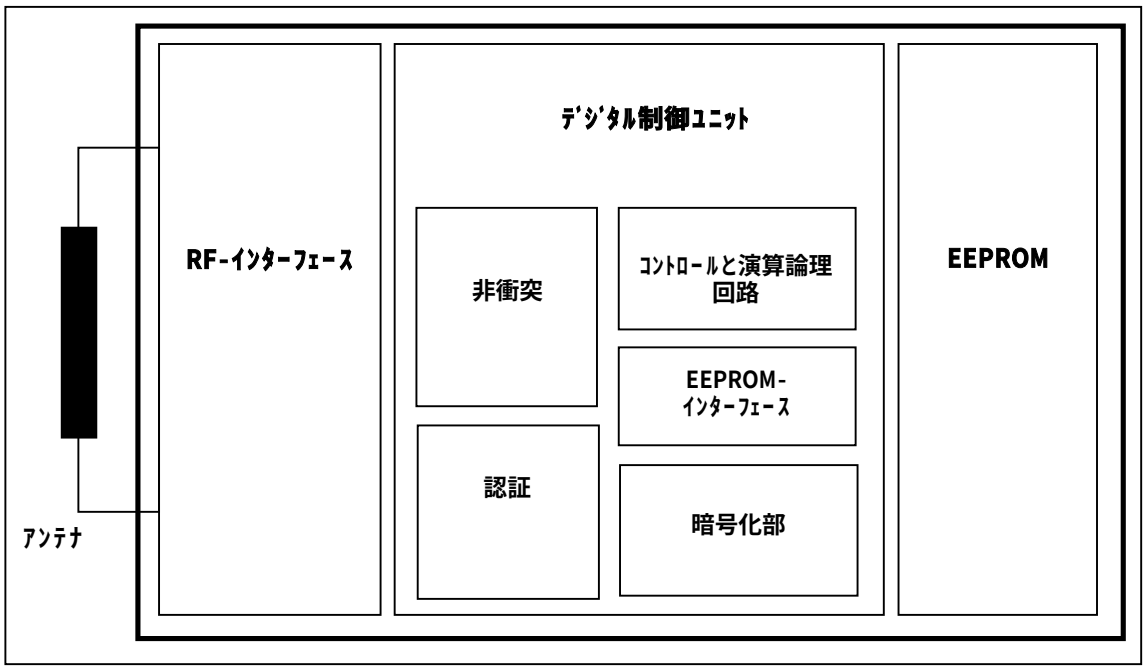


3 機能説明

3．1 ﾌﾞﾛｯｸ説明

MF1 IC S50 は1Kbyte EEPROM、 RF-ｲﾝﾀｰﾌｪｰｽ、ﾃﾞｼﾞﾀﾙ制御ﾕﾆｯﾄ から構成されます。 電源ｴﾈﾙｷﾞｰとﾃﾞｰﾀはｱﾝﾃﾅを通して伝送され、そのｱﾝﾃﾅは、MF1 IC S50 に直接接続されている2 ～ 3回巻のｺｲﾙから構成されています。これ以上の外部素子は必要ありません (ｱﾝﾃﾅﾃﾞｻﾞｲﾝに関しては、MIFARE Card IC Coil Design Guide ﾄﾞｷｭﾒﾝﾄを参照して下さい)

- RF-ｲﾝﾀｰﾌｪｰｽ
  - 変調/復調器
  - 整流器
  - ｸﾛｯｸ発生器
  - ﾊﾟﾜｰｵﾝﾘｾｯﾄ
  - 電圧ﾚｷﾞｭﾚｰﾀ
- 非衝突
  - ﾘｰﾀﾞｰ周辺の数枚のｶｰﾄﾞが選択され連続して順番に処理されます
- 認証
  - ﾒﾓﾘｰ操作に先立ち、認証手続きによりﾌﾞﾛｯｸへのｱｸｾｽは各ﾌﾞﾛｯｸで指定された二つのｷｰを通してのみ可能になります
- ｺﾝﾄﾛｰﾙと演算論理回路
  - Valueが特別な冗長ﾌｫｰﾏｯﾄで格納されており加算又は減算されます
- EEPROM-ｲﾝﾀｰﾌｪｰｽ
- 暗号化部
  - MIFARE Classic family の分野で立証済みのCRYPTO1 ｽﾄﾘｰﾑ暗号化により安全なﾃﾞｰﾀ交換が保証されます
- EEPROM
  - 1Kbyteは16ｾｸﾀｰで構成され、1ｾｸﾀｰは4ﾌﾞﾛｯｸになります。 1ﾌﾞﾛｯｸは16ﾊﾞｲﾄで構成されます。 各ｾｸﾀｰの最後尾のﾌﾞﾛｯｸはﾄﾚｲﾗｰと呼ばれ、本ｾｸﾀｰの各ﾌﾞﾛｯｸに対して二つのｷｰとﾌﾟﾛｸﾞﾗﾏﾌﾞﾙなｱｸｾｽ状態から構成されます



3．2　通信方式

ｺﾏﾝﾄﾞはRWDによって起動され相当のｾｸﾀｰに対するｱｸｾｽ状態に応じてMF1 IC S50 のﾃﾞｼﾞﾀﾙ制御ﾕﾆｯﾄ により制御されます

3．2．1　ﾘｸｴｽﾄ標準/ｵｰﾙ

ｶｰﾄﾞのﾊﾟﾜｰｵﾝﾘｾｯﾄ(POR)後、ﾘｸｴｽﾄｺﾏﾝﾄﾞに対して応答します。 RWDによりｱﾝﾃﾅ範囲内の全てのｶｰﾄﾞに送信され、ﾘｸｴｽﾄｺｰﾄﾞに対して応答します(ISO/IEC 14443A 準拠のATQA)

3．2．2　非衝突ﾙｰﾌﾟ

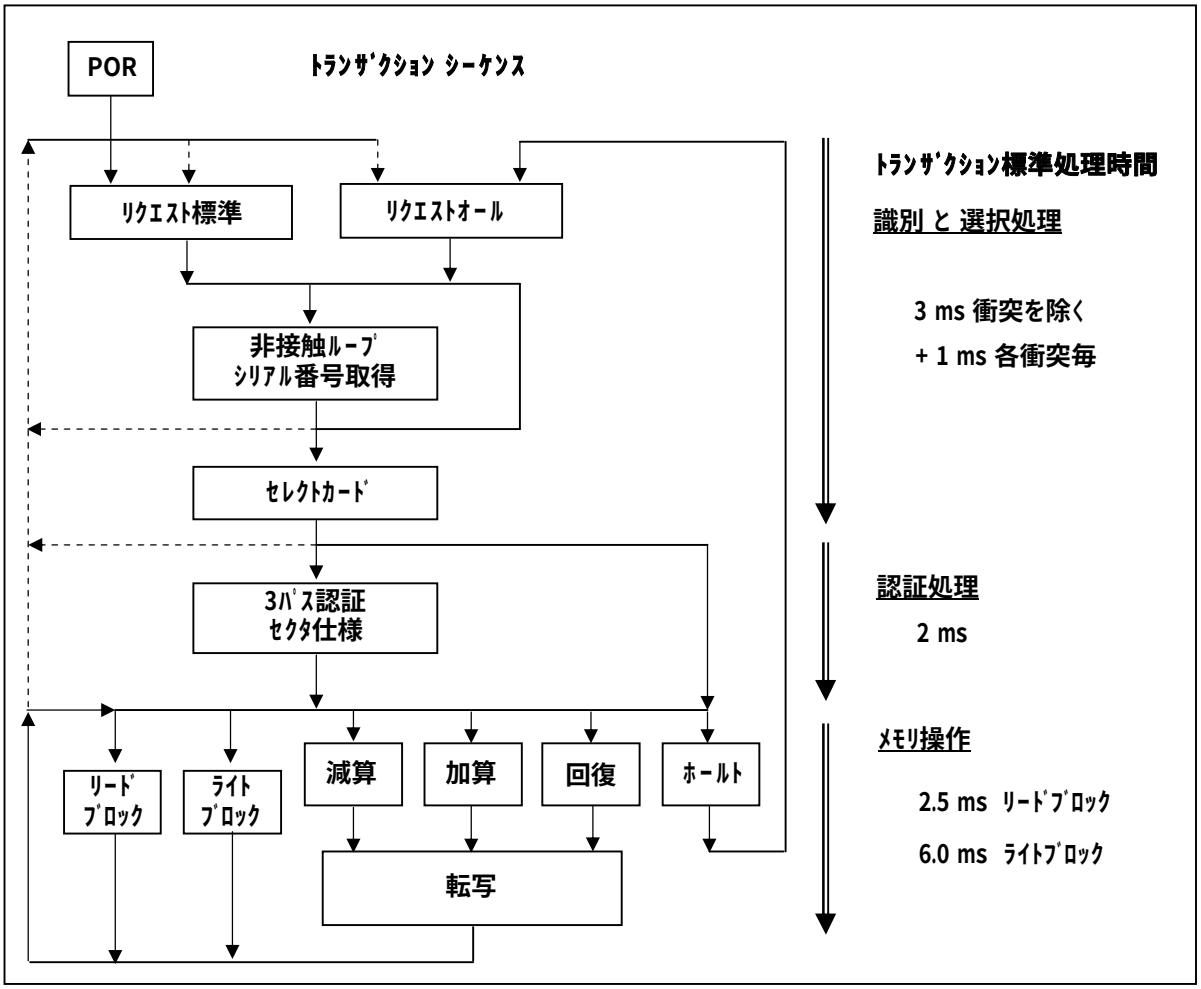
非衝突ﾙｰﾌﾟに於いて、ｶｰﾄﾞのｼﾘｱﾙ番号がﾘｰﾄﾞされます。 RWDの動作範囲内に数枚のｶｰﾄﾞが存在した場合、それらのｶｰﾄﾞはｼﾘｱﾙ番号によって区別され、1枚のみが選択され後の処理に渡されます。 選択されなかったｶｰﾄﾞはｽﾀﾝﾊﾞｲﾓｰﾄﾞに戻り、新規のﾘｸｴｽﾄｺﾏﾝﾄﾞを待ちます

3．2．3　ｾﾚｸﾄ ｶｰﾄﾞ

ｾﾚｸﾄｶｰﾄﾞｺﾏﾝﾄﾞで、RWDは認証とﾒﾓﾘｰ関連操作により単独のｶｰﾄﾞを選択します。 ｶｰﾄﾞはAnswer To Select(ATS)ｺｰﾄﾞを返し、選択ｶｰﾄﾞのﾀｲﾌﾟを決定します。 更に詳細に関しては、MIFARE Standardized Card Type Identification Procedure ﾄﾞｷｭﾒﾝﾄを参照して下さい

3．2．4　3 ﾊﾟｽ認証

ｶｰﾄﾞ選択後、RWD は次項で説明するﾒﾓﾘｰｱｸｾｽによりﾒﾓﾘｰ位置を特定し、3ﾊﾟｽ認証手順用の相当ｷｰを使用します。 認証の完了後、全てのﾒﾓﾘｰ操作は暗号化されます



3．2．5 ﾒﾓﾘ操作

認証後、下記の操作が実行されます

- ﾌﾞﾛｯｸ読出し (Read block)
- ﾌﾞﾛｯｸ書込み (Write block)
- 減算 (Decrement)
  - ﾌﾞﾛｯｸの内容を減算し、一時内部ﾃﾞｰﾀﾚｼﾞｽﾀに結果を保存します
- 加算 (Increment)
  - ﾌﾞﾛｯｸの内容を加算し、一時内部ﾃﾞｰﾀﾚｼﾞｽﾀに結果を保存します
- 回復 (Restore)
  - ﾌﾞﾛｯｸの内容をﾃﾞｰﾀﾚｼﾞｽﾀに移動します
- 転写 (Transfer)
  - 一時内部ﾃﾞｰﾀﾚｼﾞｽﾀの内容をﾊﾞﾘｭｰﾌﾞﾛｯｸに書込みます

3．3 ﾃﾞｰﾀの整合性

下記の構造はRWDとｶｰﾄﾞ間の非接触通信のﾘﾝｸ上に仕組まれており高信頼性のﾃﾞｰﾀ転送を保証しています

- 16 bits CRC /ﾌﾞﾛｯｸ
- ﾊﾟﾘﾃｨﾋﾞｯﾄ / 各ﾊﾞｲﾄ
- ﾋﾞｯﾄ数ﾁｪｯｸ
- 1', '0', 又は 'ﾉｰﾃﾞｰﾀ (情報無し)' を判別する為のﾋﾞｯﾄｺｰﾄﾞ
- ﾁｬﾈﾙﾓﾆﾀｰ (ﾌﾟﾛﾄｺﾙｼｰｹﾝｽとﾋﾞｯﾄｽﾄﾘｰﾑ解析)

3．4 安全性

高安全性ﾚﾍﾞﾙを確保する為に、ISO 9798-2準拠の3ﾊﾟｽ認証が使用されています

3．4．1 3 ﾊﾟｽ認証ｼｰｹﾝｽ

a) RWD はｱｸｾｽされるべきｾｸﾀｰを特定し、key A もしくは key B を選択します
b) ｶｰﾄﾞはｾｸﾀﾄﾚｲﾗからｼｰｸﾚｯﾄｷｰとｱｸｾｽ条件をﾘｰﾄﾞします。 それから、ｶｰﾄﾞはﾁｬﾚﾝｼﾞｺｰﾄﾞとしてのﾗﾝﾀﾞﾑ数をRWDに送ります (ﾊﾟｽ1)
c) RWDはｼｰｸﾚｯﾄｷｰと付加入力を使ってその応答ｺｰﾄﾞを計算します。 その応答は、RWDからのﾗﾝﾀﾞﾑﾁｬﾚﾝｼﾞｺｰﾄﾞと一緒にｶｰﾄﾞに送られます (ﾊﾟｽ2)
d) ｶｰﾄﾞはRWDからの応答と自身のﾁｬﾚﾝｼﾞｺｰﾄﾞを比較する事によってﾍﾞﾘﾌｧｲし、ﾁｬﾚﾝｼﾞｺｰﾄﾞに対する応答を計算してそれを送ります (ﾊﾟｽ3)
e) RWDはｶｰﾄﾞからの応答と自身のﾁｬﾚﾝｼﾞｺｰﾄﾞを比較する事によってﾍﾞﾘﾌｧｲします

最初のﾗﾝﾀﾞﾑﾁｬﾚﾝｼﾞｺｰﾄﾞの送信後、ｶｰﾄﾞとRWD間の通信は暗号化されます

3．5 RF ｲﾝﾀｰﾌｪｰｽ

RF ｲﾝﾀｰﾌｪｰｽ は非接触型ｽﾏｰﾄｶｰﾄﾞ ISO/IEC 14443A 標準に準拠しています

RWDからのｷｬﾘｱ電界は常に存在しており、ｶｰﾄﾞの電源に使用されます (送信時小休止を伴いますが)

通信の両方向に於いて、各ﾌﾚｰﾑの起動時にｽﾀｰﾄﾋﾞｯﾄは1ﾋﾞｯﾄのみです。 各ﾊﾞｲﾄは終了時にﾊﾟﾘﾃｨ付き(奇数ﾊﾟﾘﾃｨ)で送信されます。 選択されたﾌﾞﾛｯｸの最小ｱﾄﾞﾚｽのﾊﾞｲﾄのLSB が最初に送信されます。 最大のﾌﾚｰﾑ長は163ﾋﾞｯﾄになります (16 ﾀﾞｰﾀﾊﾞｲﾄ + 2 CRC ﾊﾞｲﾄ = 16 * 9 + 2 * 9 + 1 ｽﾀｰﾄﾋﾞｯﾄ)

3．6 ﾒﾓﾘ構成

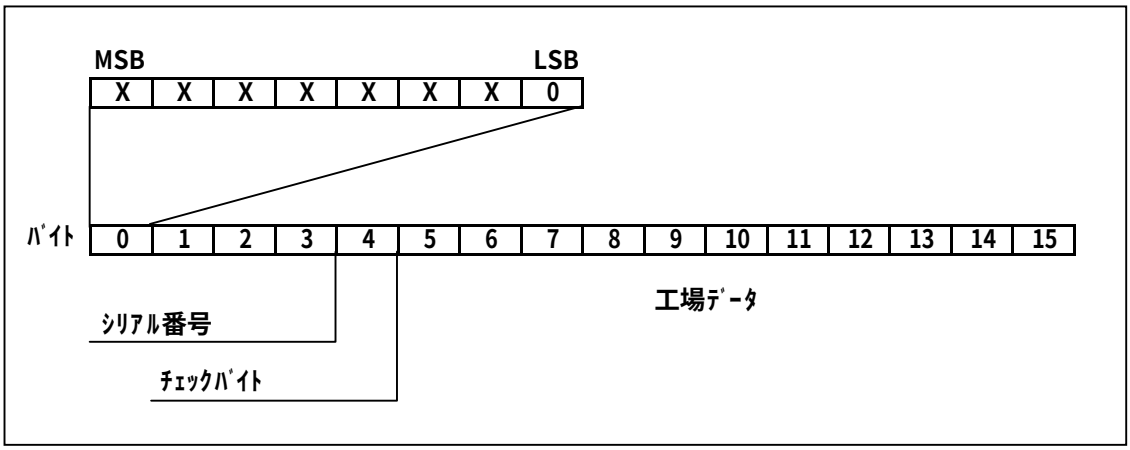
1024 x 8 bit EEPROM ﾒﾓﾘは 16 ｾｸﾀ, 4 ﾌﾞﾛｯｸ, 各ﾌﾞﾛｯｸ16 ﾊﾞｲﾄ で構成されています

ｲﾚｰｽﾞ状態に於いては、EEPROM ｾﾙは論理 '0' としてﾘｰﾄﾞされ、書込み時は論理 '1' になります

		ﾌﾞﾛｯｸ内のﾊﾞｲﾄ番号														
ｾｸﾀ	ﾌﾞﾛｯｸ	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	説明
15	3	Key A						ｱｸｾｽﾋﾞｯﾄ				Key B						ｾｸﾀﾄﾚｲﾗ No.15
	2																	ﾃﾞｰﾀ
	1																	ﾃﾞｰﾀ
	0																	ﾃﾞｰﾀ
14	3	Key A						ｱｸｾｽﾋﾞｯﾄ				Key B						ｾｸﾀﾄﾚｲﾗ No.14
	2																	ﾃﾞｰﾀ
	1																	ﾃﾞｰﾀ
	0																	ﾃﾞｰﾀ
:	:																	
:	:																	
:	:																	
1	3	Key A						ｱｸｾｽﾋﾞｯﾄ				Key B						ｾｸﾀﾄﾚｲﾗ No.1
	2																	ﾃﾞｰﾀ
	1																	ﾃﾞｰﾀ
	0																	ﾃﾞｰﾀ
0	3	Key A						ｱｸｾｽﾋﾞｯﾄ				Key B						ｾｸﾀﾄﾚｲﾗ No.0
	2																	ﾃﾞｰﾀ
	1																	ﾃﾞｰﾀ
	0																	工場ﾌﾞﾛｯｸ

3．6．1　工場ﾌﾞﾛｯｸ

これは最初のｾｸﾀ (ｾｸﾀ 0) の最初のﾃﾞｰﾀﾌﾞﾛｯｸ (ﾌﾞﾛｯｸ 0) になります。それは、IC の 工場ﾃﾞｰﾀ を含みます。安全性とｼｽﾃﾑ要件から、このﾌﾞﾛｯｸは製作時、IC 製造業者によりﾌﾟﾛｸﾞﾗﾑされた後、書込み保護されています



3．6．2　ﾃﾞｰﾀ ﾌﾞﾛｯｸ

全てのｾｸﾀは格納ﾃﾞｰﾀとして16ﾊﾞｲﾄの3 ﾌﾞﾛｯｸ から構成されています。(ｾｸﾀ 0は2 ﾃﾞｰﾀ ﾌﾞﾛｯｸのみとﾘｰﾄﾞ ｵﾝﾘの工場ﾃﾞｰﾀ から成ります)

ﾃﾞｰﾀ ﾌﾞﾛｯｸは以下のように、ｱｸｾｽﾋﾞｯﾄによって構成されます

- ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ　例として非接触ｱｸｾｽ制御です
- ﾊﾞﾘｭｰ ﾌﾞﾛｯｸ　例として電子財布ｱﾌﾟﾘｹｰｼｮﾝ (電子決済)、それは保存値の直接制御の為の 加算 とか 減算 のような付加的なｺﾏﾝﾄﾞが適用されます

認証ｺﾏﾝﾄﾞは、ﾒﾓﾘ操作に先だって実行されると次のｺﾏﾝﾄﾞが受付可能となります

3．6．2．1　ﾊﾞﾘｭｰ ﾌﾞﾛｯｸ

ﾊﾞﾘｭｰ ﾌﾞﾛｯｸにより電子財布機能を実行させる事ができます (有効なｺﾏﾝﾄﾞ：ﾘｰﾄﾞ, ﾗｲﾄ, 加算, 減算, 回復, 転写)。ﾊﾞﾘｭｰ ﾌﾞﾛｯｸは、固定ﾃﾞｰﾀﾌｫｰﾏｯﾄになっておりｴﾗｰ検出とその修正及びﾊﾞｯｸｱｯﾌﾟ管理を可能にします。ﾊﾞﾘｭｰ ﾌﾞﾛｯｸはﾊﾞﾘｭｰ ﾌﾞﾛｯｸ ﾌｫｰﾏｯﾄの書込み操作を通して生成されます

- ﾊﾞﾘｭｰ
  - 正負の4バイトの値を意味しています。ﾊﾞﾘｭｰ のLSB は最下位ｱﾄﾞﾚｽに保存されます。負のﾊﾞﾘｭｰ は標準の2の補数ﾌｫｰﾏｯﾄで保存されます。ﾃﾞｰﾀ整合性と安全の為に、ﾊﾞﾘｭｰ は3回、2回は非反転で、1回は反転で保存されます
- Adr (ｱﾄﾞﾚｽ)
  - 1 ﾊﾞｲﾄ ｱﾄﾞﾚｽを意味しており、効果的なﾊﾞｯｸｱｯﾌﾟ管理を施行する時のﾌﾞﾛｯｸの格納ｱﾄﾞﾚｽを保存するのに使用されます。ｱﾄﾞﾚｽﾊﾞｲﾄは4回、2回の反転と非反転で保存されます。加算, 減算, 回復 及び 転写 の処理中は、ｱﾄﾞﾚｽは変更されません。ﾗｲﾄ ｺﾏﾝﾄﾞを通してのみ変更可能です

ﾊﾞｲﾄ番号の説明	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ﾊﾞﾘｭｰ				ﾊﾞﾘｭｰ				ﾊﾞﾘｭｰ				Adr	$\overline{\text{Adr}}$	Adr	$\overline{\text{Adr}}$

3．6．3 ｾｸﾀ ﾄﾚｲﾗ (ﾌﾞﾛｯｸ No.3)

各ｾｸﾀｰは下記に示されるｾｸﾀｰ ﾄﾚｲﾗを有しています

- 論理 '0' で読み出される ｼｰｸﾚｯﾄ keys A と keys B(ｵﾌﾟｼｮﾝ)
- 4つのﾌﾞﾛｯｸに対するｱｸｾｽ状態は、ﾊﾞｲﾄ 6…9に保存されています
- ｱｸｾｽ ﾋﾞｯﾄはﾃﾞｰﾀ ﾌﾞﾛｯｸのﾀｲﾌﾟ (ﾘｰﾄﾞ/ﾗｲﾄ 又は ﾊﾞﾘｭｰ)をも示しています

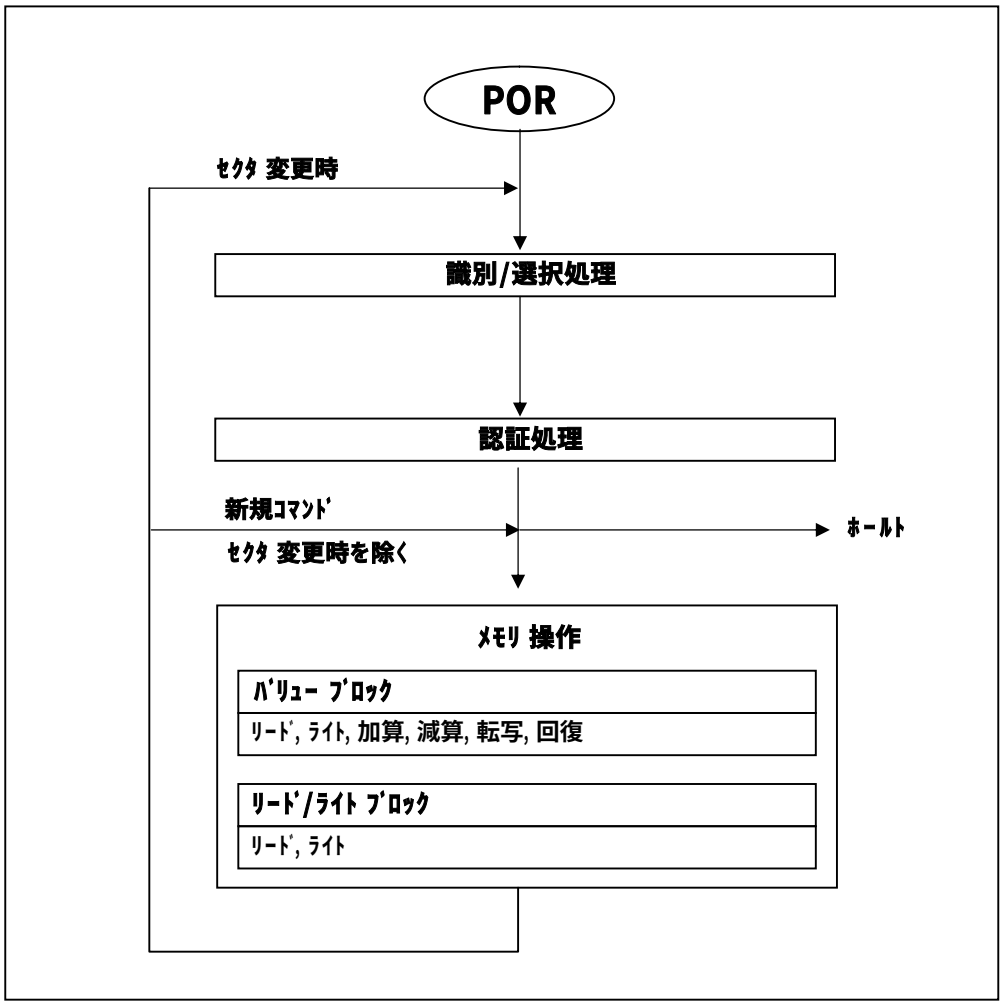
key B が必要なければ、ﾌﾞﾛｯｸNo.3 の最後の6ﾊﾞｲﾄはﾃﾞｰﾀﾊﾞｲﾄに使用されます

ｾｸﾀ ﾄﾚｲﾗの9 ﾊﾞｲﾄ目はﾕｰｻﾞ ﾊﾞｲﾄ用に有効です。 このﾊﾞｲﾄには、ﾊﾞｲﾄ 6、7、および8と同じｱｸｾｽ権を適用してください。

ﾊﾞｲﾄ番号の説明	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Key A						ｱｸｾｽﾋﾞｯﾄ				Key B (ｵﾌﾟｼｮﾝ)					

3．7 ﾒﾓﾘｱｸｾｽ

ﾒﾓﾘ操作が実行される前に、ｶｰﾄﾞは前に説明したように選択された後、認証されなければなりません。 指定されたﾌﾞﾛｯｸに対する有効なﾒﾓﾘ操作は該当するｾｸﾀﾄﾚｲﾗに格納されているｷｰとｱｸｾｽ条件に依存します



ﾒﾓﾘ操作		
処理名	説明	ﾌﾞﾛｯｸﾀｲﾌﾟの有効処理
ﾘｰﾄﾞ (Read)	ﾒﾓﾘ ﾌﾞﾛｯｸをﾘｰﾄﾞする	ﾊﾞﾘｭｰ と ｾｸﾀ ﾄﾚｲﾗ のﾘｰﾄﾞ/ﾗｲﾄ
ﾗｲﾄ (Write)	ﾒﾓﾘ ﾌﾞﾛｯｸをﾗｲﾄする	ﾊﾞﾘｭｰ と ｾｸﾀ ﾄﾚｲﾗ のﾘｰﾄﾞ/ﾗｲﾄ
加算 (Increment)	ﾌﾞﾛｯｸの内容を加算し内部ﾃﾞｰﾀﾚｼﾞｽﾀに結果を保存する	ﾊﾞﾘｭｰ
減算 (Decrement)	ﾌﾞﾛｯｸの内容を減算し内部ﾃﾞｰﾀﾚｼﾞｽﾀに結果を保存する	ﾊﾞﾘｭｰ
転写 (Transfer)	内部ﾃﾞｰﾀ ﾚｼﾞｽﾀの内容をﾌﾞﾛｯｸに書き込む	ﾊﾞﾘｭｰ
回復 (Restore)	ﾌﾞﾛｯｸの内容を内部ﾃﾞｰﾀﾚｼﾞｽﾀに読み込む	ﾊﾞﾘｭｰ

3．7．1 ｱｸｾｽ状態

各ﾃﾞｰﾀ ﾌﾞﾛｯｸとｾｸﾀ ﾄﾚｲﾗのｱｸｾｽ状態は、3ﾋﾞｯﾄで決められ、指定ｾｸﾀのｾｸﾀﾄﾚｲﾗ上に非反転と反転で保存されています

ｱｸｾｽﾋﾞｯﾄはｼｰｸﾚｯﾄ key A と key B を使って、ﾒﾓﾘｱｸｾｽ権を制御します。 関連ｷｰを認識していて、現在のｱｸｾｽ状態がその操作を可能にしているのであれば、ｱｸｾｽ状態は変更されるかもしれません

注： 下記の説明に於いて、ｱｸｾｽﾋﾞｯﾄは非反転ﾓｰﾄﾞのみとして言及されています

MF1 IC S50の内部ﾛｼﾞｯｸは、ｺﾏﾝﾄﾞが認証手順の後にだけ実行され、さもなければ実行されないことを確実にします

ｱｸｾｽ ﾋﾞｯﾄ	有効なｺﾏﾝﾄﾞ		ﾌﾞﾛｯｸ	説明
$C1_3$, $C2_3$, $C3_3$	ﾘｰﾄﾞ, ﾗｲﾄ	->	3	ｾｸﾀ ﾄﾚｲﾗ
$C1_2$, $C2_2$, $C3_2$	ﾘｰﾄﾞ, ﾗｲﾄ, 加算, 減算, 転写, 回復	->	2	ﾃﾞｰﾀ ﾌﾞﾛｯｸ
$C1_1$, $C2_1$, $C3_1$	ﾘｰﾄﾞ, ﾗｲﾄ, 加算, 減算, 転写, 回復	->	1	ﾃﾞｰﾀ ﾌﾞﾛｯｸ
$C1_0$, $C2_0$, $C3_0$	ﾘｰﾄﾞ, ﾗｲﾄ, 加算, 減算, 転写, 回復	->	0	ﾃﾞｰﾀ ﾌﾞﾛｯｸ

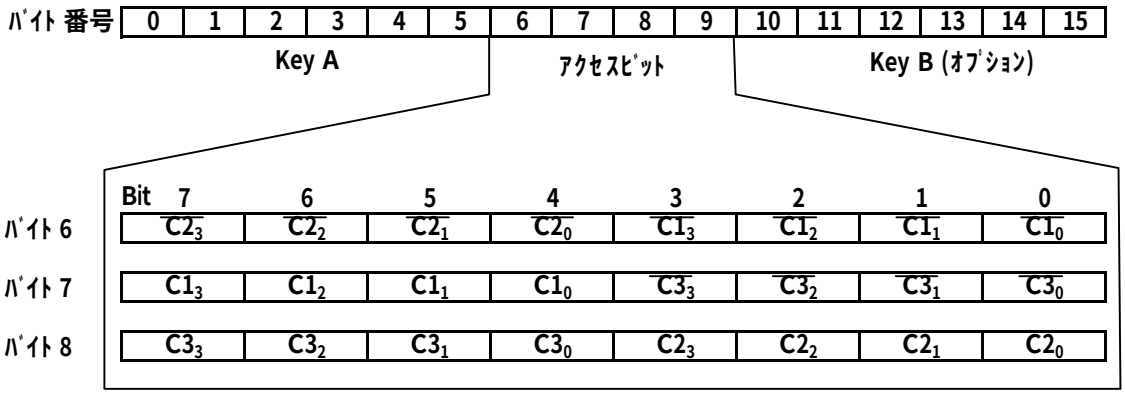
注： 各ﾒﾓﾘ ｱｸｾｽに於いて、内部論理回路はｱｸｾｽ状態のﾌｫｰﾏｯﾄを精査します。 ﾌｫｰﾏｯﾄ違反があれば、全体のｾｸﾀは回復不能なｾｸﾀになります

3．7．2 ｾｸﾀ ﾄﾚｲﾗに対するｱｸｾｽ状態

ｾｸﾀ ﾄﾚｲﾗ (ﾌﾞﾛｯｸ No.3)上のｱｸｾｽ ﾋﾞｯﾄにより、ｷｰとｱｸｾｽ ﾋﾞｯﾄに対する ﾘｰﾄﾞ/ﾗｲﾄ ｱｸｾｽは、'never', 'key A', 'key B' もしくは'key A|B' (key A or key B) として指定されます

ﾁｯﾌﾟ出荷時に、ｾｸﾀ ﾄﾚｲﾗと key A のｱｸｾｽ状態が輸送構成として予め定義されます。 key B が輸送構成時に読出しされるかもしれないので、新規ｶｰﾄﾞは、key A で認証されなければならないということです。

ｱｸｾｽﾋﾞｯﾄ自身もまた、妨害されることもあるので、特別の注意がｶｰﾄﾞの個別化中に払わなければなりません



注: 灰色でﾏｰｸされた行は、key B が読出し可能で、ﾃﾞｰﾀに使用されても良いｱｸｾｽ状態です

ｱｸｾｽﾋﾞｯﾄ			ｱｸｾｽ状態						備考
			KEY A		ｱｸｾｽ ﾋﾞｯﾄ		KEY B		
C1	C2	C3	ﾘｰﾄﾞ	ﾗｲﾄ	ﾘｰﾄﾞ	ﾗｲﾄ	ﾘｰﾄﾞ	ﾗｲﾄ	
0	0	0	never	key A	key A	never	key A	key A	Key B が読出し可能
0	1	0	never	never	key A	never	key A	never	Key B が読出し可能
1	0	0	never	key B	key A|B	never	never	key B	
1	1	0	never	never	key A|B	never	never	never	
0	0	1	never	key A	key A	key A	key A	key A	Key B が読出し可能 輸送構成
0	1	1	never	key B	key A|B	key B	never	key B	
1	0	1	never	never	key A|B	key B	never	never	
1	1	1	never	never	key A|B	never	never	never	

3．7．3 ﾃﾞｰﾀﾌﾞﾛｯｸのｱｸｾｽ状態

ﾃﾞｰﾀﾌﾞﾛｯｸ(ﾌﾞﾛｯｸ 0…2)に対するｱｸｾｽﾋﾞｯﾄにより、ﾘｰﾄﾞ/ﾗｲﾄ ｱｸｾｽは 'never', 'key A', 'key B' もしくは 'key A|B' (key A 又は key B) として指定されます。関連のｱｸｾｽﾋﾞｯﾄの設定はｱﾌﾟﾘｹｰｼｮﾝと相当の適用ｺﾏﾝﾄﾞを定義します

- ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ:
  - 読出しと書込み操作が可能です
- ﾊﾞﾘｭｰ ﾌﾞﾛｯｸ:
  - 付加的な操作の 加算, 減算, 転写 及び 回復 が可能です。"001' のｹｰｽとして、再充電可能ｶｰﾄﾞにとってﾘｰﾄﾞ と 減算 のみがになります。 "110'というｹｰｽに於いては、充電が key B を使用する事によって可能になります
- 工場ﾌﾞﾛｯｸ:
  - 読出しのみの状態は、ｱｸｾｽﾋﾞｯﾄ設定の影響を受けません

- ｷｰ管理:
  - 輸送構成に於いて、key A は認証の為に使用されなければなりません (***1**)

ｱｸｾｽﾋﾞｯﾄ			ｱｸｾｽ状態				適用
C1	C2	C3	ﾘｰﾄﾞ	ﾗｲﾄ	加算	減算 転写 回復	
0	0	0	key A|B(*1)	key A|B(*1)	key A|B(*1)	key A|B(*1)	輸送構成
0	1	0	key A|B(*1)	never	never	never	ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ
1	0	0	key A|B(*1)	key B(*1)	never	never	ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ
1	1	0	key A|B(*1)	key B(*1)	key B(*1)	key A|B(*1)	ﾊﾞﾘｭｰ ﾌﾞﾛｯｸ
0	0	1	key A|B(*1)	never	never	key A|B(*1)	ﾊﾞﾘｭｰ ﾌﾞﾛｯｸ
0	1	1	key B(*1)	key B(*1)	never	never	ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ
1	0	1	key B(*1)	never	never	never	ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ
1	1	1	never	never	never	never	ﾘｰﾄﾞ/ﾗｲﾄ ﾌﾞﾛｯｸ

注(***1**): Key B が該当のｾｸﾀ ﾄﾚｲﾗで読みだされた場合は、それは認証用に使われる事はありません。(上記のﾃｰﾌﾞﾙの灰色の行)
結論: 灰色でﾏｰｸされたｱｸｾｽ状態を使って KEY B によってRWDがｾｸﾀ内のﾌﾞﾛｯｸを認証しようとした場合、ｶｰﾄﾞは認証の後、いかなるﾒﾓﾘｱｸｾｽも受けつける事はありません

4 定義

ﾃﾞｰﾀｼｰﾄの定義	
目標仕様	このﾃﾞｰﾀｼｰﾄは製品開発の為の目的もしくは目標仕様を包含しています
暫定仕様	このﾃﾞｰﾀｼｰﾄは暫定仕様を包含しています 補足のﾃﾞｰﾀが後に公開されます
製品仕様	このﾃﾞｰﾀ仕様は最終的な製品仕様を包含しています
制限値	
表記の制限値は絶対最大値評定ｼｽﾃﾑ(IEC 134)に準じています。制限値を超えるｽﾄﾚｽはﾃﾞﾊﾞｲｽに永久的なﾀﾞﾒｰｼﾞを加えることになります。この制限値はｽﾄﾚｽ評定のみを意味しており、特性仕様部で記されている制限値又はその制限値を超える状態でのﾃﾞﾊﾞｲｽの動作まで言及しておりません。定格時間を超えて制限値にさらすことはﾃﾞﾊﾞｲｽの信頼性に影響を与える可能性があります	
ｱﾌﾟﾘｹｰｼｮﾝ情報	
ｱﾌﾟﾘｹｰｼｮﾝ情報が発行される場合は、それは参考情報であり、仕様に影響する事はありません	

5 生命維持ｱﾌﾟﾘｹｰｼｮﾝ

誤動作が人の傷害に至るような生命維持の電化製品とかｼｽﾃﾑとかの使用に耐えるように設計されておりません。 そのようなｱﾌﾟﾘｹｰｼｮﾝで本製品を使用したり売ったりしたﾕｰｻﾞは自分自身のﾘｽｸを負うことになり、そのような不適当な使用又は販売から起因する損害賠償をﾌｨﾘｯﾌﾟｽ社に補償する事に同意したということになります

6 変更履歴

表1 MF1 IC S50 の機能仕様の変更履歴

改訂	月日	CPCN	頁	内容
5.1	0501	2001 05013	9,10	工場ﾌﾟﾛｯｸ の新ｺｰﾄﾞ化
5.0	1199			ﾚｲｱｳﾄ変更
1.0		-		初版