漢字 FlashROM 初回ロット不具合の調査報告

当方（にが HP）より家電の KEN ちゃんさんの委託販売にてリリースさせていただきました「漢字 FlashROM」に不具合が発覚しました。松下 12 ドット漢字 ROM 搭載機との併用で動作不良を生じる可能性があり、同フォントを利用することを前提に作られたソフトウエアで漢字 FlashROM のフォントデータが読み出せなくなる現象が発生します。調査の結果、故障を誘発するバス競合は発生しないことが判明しましたが、動作不良を起こす可能性はあり、対象となる製品を回収し、不具合が発生しないよう CPLD を書き換えて返送することにいたします。ご迷惑をおかけして申し訳ございません。

1. 機器

漢字 FlashROM と下記との併用、または松下 12 ドット漢字 ROM に対応したソフトウエアの利用

- モデムカートリッジ　FS-CM1
- MSX2 本体 FS-4600F
- MSX2 本体 FS-A1FM

「ワープロプリンタ　FS-PW1　カートリッジ」はその後の調査で松下 12 ドット漢字 ROM 非搭載と判明しました。

2. 事象

当方サークル「にが HP」より、MSX 用同人ハードウエア「漢字 FlashROM」を 2021 年 9 月 25 日に家電の KEN ちゃんさんを通じて頒布開始しました。同 9 月 30 日、基板単体 7 枚とケース入り基板 2 個の合計 9 個を売り上げた時点で、松下 12 ドット漢字 ROM が、漢字 FlashROM と同じ拡張 IO のデバイス ID で有効化されるという情報を確認しました。

同日、漢字 FlashROM を、MegaFlashROM SCC+SD を併用した際に、漢字 FlashROM のフォントを読み出せないとの報告を認めました。

ハードウエア的なバス競合が発生すると故障の原因となりうるため、直ちに家電の KEN ちゃんさん担当 HRD 氏に販売休止の措置をお願いし、当方 WEB サイトのトップページ、およびサポートページ http://niga2.sytes.net/sp/index.html に注意喚起文をリンクし、HRD 氏のツイート https://twitter.com/zan2zanjp/status/1443521668060618753 により告知を行いました。

実際にバス競合を起こす可能性や、不具合の発生条件を明らかにするため、対象機器を所有されている nf_ban 氏、れふてぃ氏の協力により、対象機器において拡張 IO レジスタを操作した時の挙動を調べ、不具合が発生する可能性のある状況を絞り込みました。

調査結果を踏まえ、漢字 FlashROM の拡張 IO 操作の手順を見直し、CPLD ファームウエアの改修を行いました。

3. 原因

初回ロットの漢字 FlashROM では書き換えモードとして下記 IO アドレスを使用していました。

IO アドレス	R/W	役割
#40h	W	36h/76h/B6h/F6h のいずれかの書き込みで第一水準書き換えモード 37h/77h/B7h/F7h のいずれかの書き込みで第二水準書き換えモード 上記以外の値の書き込みで通常モード
#41h	R/W	FlashROM の読み書き
#42h	W	FlashROM のアドレス下位 5bit 指定
#D8h	W	漢字コード下位 6bit 指定
#D9h	W	漢字コード上位 6bit 指定

書き換えモードに遷移すると、通常の漢字 ROM としての IO アドレス#D9h,DBh を介したフォントデータの読み出しはできなくなります。

ソフトウエア的には IO アドレス#40h に 36h を書き込んで第一水準書き換え、37h を書き込んで第二水準書き換えモードに遷移する仕様でしたが、CPLD リソース（GPIO ピン数）の都合により、書き込まれた値の上位 2bit は無視され、実質的に 8 通りの書き換えモードに遷移するパターンが想定されます。

システム設計時には WEB で確認できる情報によりこれらのデバイス ID が過去のハードウエアで使用されていないことを確認した上で漢字 FlashROM に実装しましたが、松下 12 ドット漢字 ROM の仕様を確認するに至りませんでした。頒布開始後にネットで松下 12 ドットフォントが拡張 IO 経由でアクセスしているという情報が流れていることを知り、下記 GitHub のアーカイブ内のテキスト文書、およびプログラムのソースにより、松下 12 ドット漢字 ROM デバイス ID が「F7h」に定義されていることを確認しました。

https://github.com/nfban/gigamix-msx/tree/master/dm-system2/font-driver/FNT-CM1X

このデバイス ID「F7h」については、過去の公式文献（MSX2 テクニカルハンドブック、MSX-Datapack）や海外の同人ハードウエアを網羅した IO 一覧表にも記載されていないものでした。漢字 FlashROM のデバイス ID として設定した「36h,37h」は下位 6bit が過去のハードウエアと被らないように決めたものでしたが、37h の下位 6bit が偶然松下 12 ドット漢字 ROM の ID「F7h」と重なったことになります。とはいえ、拡張 IO のデバイス ID は本来勝手に定義して使ってはいけないものであり、8 通りものID 書き込みでモード遷移してしまい、通常アクセスができなくなる仕組み自体に無理があったと言わざるを得ません。

2021 年 9 月現在は、松下 12 ドット漢字 ROM の仕様に不明な点が多くありましたが、nf_ban 氏、ごりぽん氏、れふてぃ氏の調査・協力により、下記仕様であることが明らかとなりました。

IO アドレス	R/W	役割
#40h	R/W	F7h 書き込みでデバイス enable（内蔵機・外付けカートリッジ共通） FS-CM1 のみ、デバイス有効時に読み取ると「08h」を返す
#41h	R	FS-CM1 タイプのデバイスに第二水準フォントが存在する場合に読み取ると「08h」を返す仕様らしいが、そのようなハードウエアは存在が確認されていない
#42h	W	本体内蔵機（FS-4600F,FS-A1FM）のみ実装されている bit0=1 で第一水準漢字が enable bit1=1 で第二水準漢字が enable になる仕様らしいが、そのようなハードウエアは存在が確認されていない
#47h	W	漢字コード上位 8bit 指定
#48h	W	漢字コード下位 8bit 指定
#49h	R	フォントデータの読み出し

漢字 FlashROM の書き込みモードと松下 12 ドット漢字 ROM はいずれも IO アドレス#40h に F7h を書き込むことで有効化されますが、バス競合は複数のハードウエアが異なるデータを同一の IO ポートに出力した場合に発生します。今回の事例では#41h の読み出しでバス競合の懸念がありますが、松下 12 ドット漢字 ROM では FS-CM1 タイプにおいて第二水準フォントが搭載されている場合のみ#41h から 08h を出力する仕様になっているようです。2021 年現在このようなカートリッジの存在は確認されておらず、実質的にバス競合を発生させるデバイスは存在しません。したがって、漢字 FlashROM と松下 12 ドット漢字 ROM 搭載ハードウエアを併用しても、故障の原因になりうるバス競合は発生しないと結論づけました。

漢字 FlashROM と上記デバイスの併用において動作不良が発生する状況としては、松下 12 ドット漢字 ROM の存在確認プログラムにおいて IO アドレス#41h を読み取った結果、漢字 FlashROM が偶然 08h（値は直前に読み取った漢字コードに依存）を返し、本体内蔵タイプの第二水準松下 12 ドット漢字 ROM が存在すると誤認する可能性や、12 ドットフォント使用中に漢字 FlashROM のフォントが読めなくなる事象が予想されますが、通常の使用において発生頻度は低いと思われます。

上記デバイスと併用しない場合でも、松下 12 ドット漢字 ROM を利用することを前提に作られたソフトウエアにおいて、漢字 FlashROM が意図せずに書き換えモードに遷移し、漢字フォントデータが読み出せなくなる事象は発生します。

なお、漢字 FlashROM の書き換えは複雑なコマンドシーケンスに則って行う必要があり、偶然に消去コマンドが発行されたり、データが書き換わってしまう確率は無視できます。したがって FlashROM の内容が破壊される可能性はほぼありません。

4. 対処

下記のように漢字 FlashROM の書き換えモードへ遷移する手順を変更しました。

IO アドレス	R/W	役割
#40h	W	**27h-36h-39h-0 を順番に書き込むと第一水準書き換えモード** **第一水準書き換えモードから更に 0 を書き込むと第二水準書き換えモード** **第二水準書き換えモードから更に 0 を書き込むと通常モード** **#40h を読み出すか、上記以外の値の書き込みで通常モード**
#41h	R/W	FlashROM の読み書き
#42h	W	FlashROM のアドレス下位 5bit 指定
#D8h	W	漢字コード下位 6bit 指定
#D9h	W	漢字コード上位 6bit 指定

4 段階のコマンドシーケンスになっており、IO アドレス#40h に 3 つの特定値を順番に書き込み、次いで 0 を書き込むことで書き替えモードに遷移します。書き込みデータの上位 2bit は無視されますので、6bit x3=18bit の暗号ロックと同等のセキュリティとなっています。#40h を読み出したり、特定値以外の値を書き込んだ時はコマンドシーケンスがリセットされ、最初からやり直さなければなりません。最終的に#40h へ 0 を書き込むことでモード遷移しますが、拡張 IO のデバイス ID として 0 と 255 は使用しないと MSX-Datapack（Appendix A.5 拡張 I/O ポート）に明記されていることから、既存の拡張 IO デバイスとの競合は発生しません。また、今後誰かが同様のシーケンスにより有効化される拡張 IO デバイスを作った場合でも、偶然 ID が一致してしまう確率は 1/262144 と極めて低い水準です。

2021 年 10 月以降の製品につきましては CPLD 内部ロジックを上記仕様に設定して頒布いたします。同 9 月に頒布した漢字 FlashROM につきましては郵送での改修を受け付けますので、下記 blog 記事の手順に従ってお申し込みください。勝手ながら期限を 2021 年内とさせていただきます。Xilinx の CPLD 書き込み環境をお持ちの方はファームウエア（JED ファイル）を同 blog 内からダウンロードできますので、ご自身で書き換えて頂いても結構です。

漢字 FlashROM　初期ロット改修について　（にが Blog2）

5. 知識化

MSX のシステムで定義されている IO アドレスや拡張機器のデバイス ID は、本来重複が発生しないように管理されるべきものですが、2021 年現在は管理団体が存在しません。既存の MSX の拡張ハードウエアには、仕様が公開されていないものがあり、新規ハードウエアの開発において迂闊に IO アドレスやデバイス ID を定義・使用をすると、未知のデバイスと競合を起こしたり、思わぬ動作不良を引き起こす恐れがあります。今回の出来事が今後の同人ハード開発にあたっての教訓になればと思います。

作者の WEB サイト：にが HP　http://niga2.sytes.net