

PalmOS 上でのマクロウイルスの動作実験  
結果報告書

平成 13 年 2 月

情報処理振興事業協会

# 目次

1	はじめに.....	1
2	背景と目的.....	3
3	PalmOS での感染実験.....	4
3.1	XM/Laroux.....	7
3.1.1	ファイル転送.....	7
3.1.2	メールへの添付(HotSync による送受信).....	9
3.1.3	メールへの添付(直接送受信).....	9
3.2	W97M/X97M/P97M/Tristate.....	10
3.2.1	ファイル転送.....	10
3.3	W97M/Class.....	12
3.3.1	ファイル転送.....	12
3.4	W97M/Marker.....	15
3.4.1	ファイル転送.....	15
3.5	W97M/Ethan.....	17
3.5.1	ファイル転送.....	17
4	実験結果の考察.....	19
4.1	PalmOS 用アプリケーションソフトの機能について.....	20
4.2	ファイル変換について.....	21
4.3	メール添付について.....	22
5	まとめ.....	23

# 1 はじめに

本報告書は、携帯コンピュータ用の OS として注目されつつある PalmOS 上において、現在パーソナルコンピュータ用の OS である Windows 95/98 等で問題となっている代表的なマクロウイルスの動作実験を行い、PalmOS 環境におけるマクロウイルスの危険性を検証し、その結果を報告するものである。

実験対象とするマクロウイルスは以下の 5 種類である。

- XM/Laroux
- W97M/X97M/P97M/Tristate
- W97M/Class
- W97M/Marker
- W97M/Ethan

実験に用いた PalmPowered ハンドヘルド<sup>1</sup>は現在入手可能な以下の 2 種類としたが、PalmOS のバージョンはすべて同じであり、実験結果も同一のものとなった。なお、本報告書ではこれらの端末を PalmOS マシンまたは単に Palm と呼ぶ。

- IBM 社製 WorkPad c3、Palm OS Version 3.5 日本語版、RAM 8MB、モノクロモデル



<sup>1</sup> 「PalmPowered ハンドヘルド」は、PalmOS を搭載したハンドヘルド機の総称。

- SONY 社製 CLIE PEG-S500C、PalmOS Version 3.5 日本語版、RAM 8MB、カラーモデル



## 2 背景と目的

コンピュータウイルス(以下ウイルスと呼ぶ)とは、自分自身のコピーを他のプログラムに追加(感染)することで自己増殖するプログラムである。ウイルスは、その感染プログラムの移動によってあるマシンから他のマシンへと拡散していき、また、ある条件であらかじめ決められている動作を起こし(発病)、システムに深刻な被害をもたらすことがある。近年、携帯端末機器でインターネットや電子メールを利用する機会が増え、携帯端末機器でもコンピュータウイルスに遭遇するケースが増えている。

Microsoft Windows 95/98 等では、Microsoft Office 系アプリケーションソフトウェア上で動作するマクロウイルスが猛威を振るっており、それらのファイルを扱うことのできる携帯端末機器でもウイルスの感染が懸念されている。特に、代表的な携帯端末機器である PalmOS マシン用に Microsoft Office 系のアプリケーションとデータの互換性を持つソフトウェアが販売されているが、それらを用いた場合の PalmOS 上でのマクロウイルスの動作は明らかにされておらず、どのような影響が出るかも不明である。

本実験は、Microsoft Office とデータを交換することが可能な PalmOS 用アプリケーションソフトウェアの機能を調査し、マクロウイルスの動作確認やその被害が及ぶ範囲を明らかにするものであり、その結果を、PalmOS に関連したウイルス対策を構築するための基礎資料とすることを目的としている。

### 3 PalmOS での感染実験

実験に用いた PalmOS マシンは IBM 社製の WorkPad と SONY 社製の CLIE であり、その OS である PalmOS のバージョンはどれも 3.5 である。

PalmOS マシンにインストールされている標準アプリケーションは Microsoft Office のファイルをサポートしておらず、直接 Office ファイルを操作することはできなかった。しかし、Office ファイルを扱うことのできる PalmOS 用アプリケーションが市販されていることがわかった。そこで今回は、存在を確認した 2 種類のアプリケーション、Cutting Edge Software 社製 Quickoffice Version 5.0 の Quickword と Quicksheet および DataViz 社製 Documents To Go Professional Edition Version 3.0 の WordToGo と SheetToGo を取り上げ、実験に使用した。これらは、PalmOS 上で Microsoft Word と Microsoft Excel のファイルを作成・閲覧・編集可能にするソフトウェアである<sup>2</sup>。ただし、PalmOS マシン側のアプリケーションとデータを交換する際はファイル変換が必要であり、PC 側のアプリケーションがそれを行う。

実験を行うマクロウイルスは XM/Laroux、W97M/X97M/P97M/Tristate、W97M/Class、W97M/Marker、W97M/Ethan の 5 種類とする。なお、Tristate は Excel ファイルに感染した状態のものをを用いた。

パーソナルコンピュータ(PC)と携帯端末とでファイルを転送するために、PC 側に HotSync Version 3.5 をインストールし、両者をシリアルケーブル<sup>3</sup>で接続して通信を行った。また、電子メールの取り扱いには PalmOS の標準メールアプリケーションと Microsoft Exchange の受信トレイを利用した。受信トレイは PC の Windows 95/98 に付属している、添付ファイルを扱うことのできる標準的な電子メールソフトウェアである。また、携帯電話を用いた直接メール送受信のためには Palm 社製の MultiMail Professional Version 2.26J を利用した。

以上により、PalmOS マシン上で動作する Quickword、Quicksheet、WordToGo、SheetToGo の 4 種類のアプリケーション上で上記ウイルスの動作実験を行う。

---

<sup>2</sup> どちらも Microsoft PowerPoint のファイルには未対応。

<sup>3</sup> CLIE では USB ケーブルを用いた。

## 実験手順 Quickoffice の場合

1. PC 側の Quickoffice Desktop で"Quicksheet"または"Quickword"を選択し、"Add Document..."ボタンで対象ファイル(\*.doc / \*.xls)をリストに追加する(図 1)。この操作でファイルは PalmOS 用の形式(\*.qwd / \*.qsh)に変換される。

**自動実行マクロが動作することに注意。それがウイルスであれば感染する。**

2. その際、元のファイルにリンクさせるかどうかの確認があるが(図 2)、リンクさせると、PalmOS マシンで更新したデータを PC に戻したときに、自動的に PC 上の元のファイルが更新される。今回はリンクさせて実験した。
3. HotSync にて PalmOS 用ファイルを PalmOS マシンに転送する。
4. PalmOS マシン側で Quicksheet または Quickword を起動し、受信したファイルを開いてその挙動を確認し、その後データの内容を更新して保存する。
5. HotSync にて更新したファイルを PC に転送する。

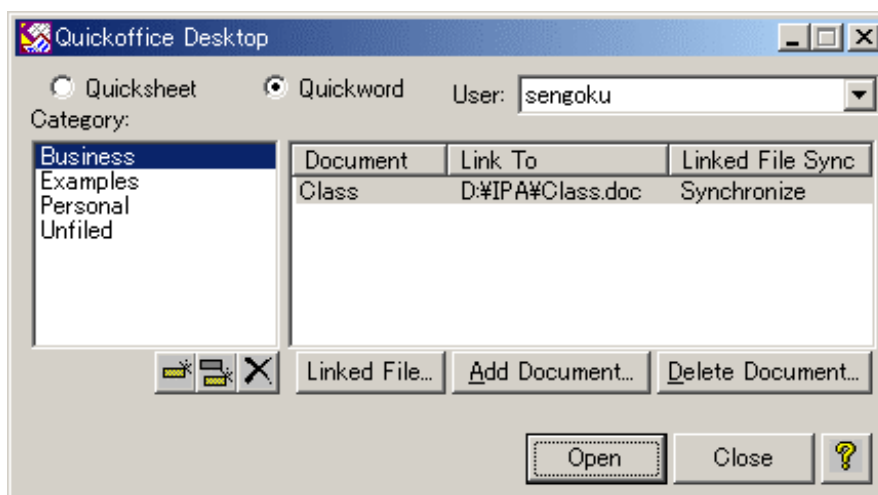


図1 : Quickoffice Desktop

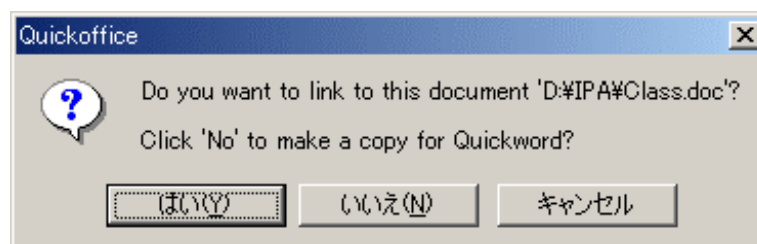


図2 : リンクの確認

## 実験手順 Documents To Go の場合

1. PC 側の Documents To Go プログラムの "Add Item" ボタンで対象ファイル (\*.doc / \*.xls) をリストに追加する(図 3)。この操作でファイルは PalmOS 用の形式 (\*.pdb) に変換される。この際、自動的に元のファイルとリンクされる。
2. HotSync にて PalmOS 用ファイルを PalmOS マシンに転送する。
3. PalmOS マシン側で SheetToGo または WordToGo を起動し、受信したファイルを開いてその挙動を確認し、その後データの内容を更新して保存する。
4. HotSync にて更新したファイルを PC に転送する。

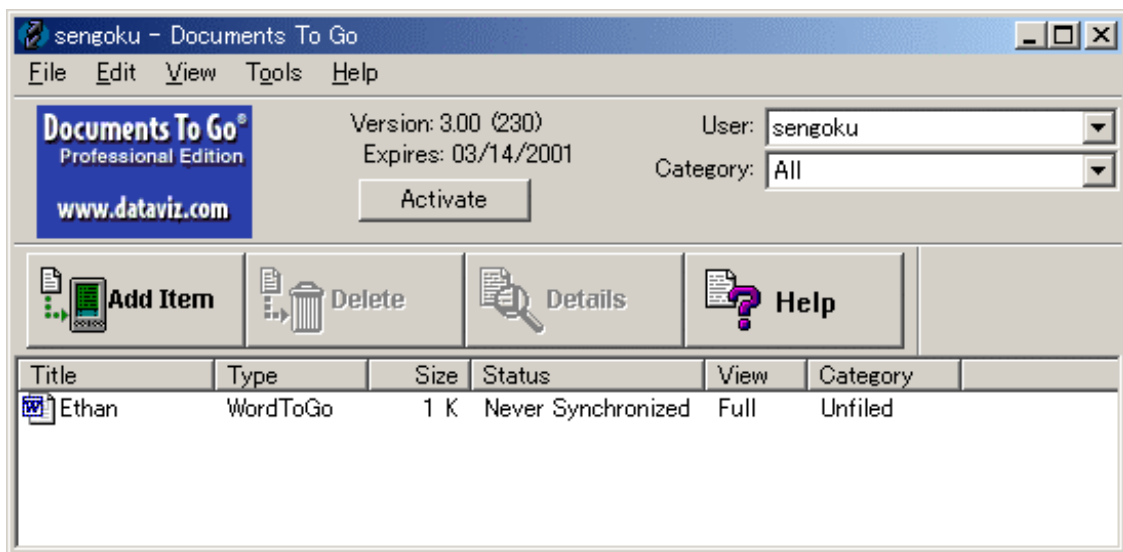


図3 : Documents To Go メイン画面



### 3.1 XM/Laroux

Laroux は Microsoft Excel で動作するマクロウイルスである。ここでは、Laroux ウィルスに感染している "Laroux.xls" を検体とし、Excel データを扱うことのできる Quicksheet と SheetToGo で開いたときの動作を調査する。

#### 3.1.1 ファイル転送

Quicksheet -----

パーソナルコンピュータ(以下 PC と表記する)側の Quickoffice Desktop でファイル形式を変換し、HotSync で PC と PalmOS マシン(以下 Palm と表記する)との間でファイル転送を行った。

PC: Laroux.xls (17.5KB)    PC: Laroux.qsh (2.1KB)  
PC: Laroux.qsh (2.1KB)    Palm: Laroux (23B)

PC 上でのファイル形式の変換<sup>4</sup>の時点で拡張子が "qsh" となり、ファイルサイズが大幅に減少した。変換後の qsh ファイルはテキストファイルであり、元の xls ファイルへのリンク情報や数値・計算式のデータが格納されていたが、マクロコードは存在しなかった。

ただし、ファイル形式の変換の際、バックグラウンドで Excel が起動して対象ファイルが読み込まれ、そのファイルデータを基に qsh 形式のファイルが生成されるのだが、この時点で自動実行ウイルスマクロが動作し PC が感染してしまう。これは Excel のセキュリティレベルに関係なく実行されるため注意が必要である。また、Excel でファイルを開くときのウイルス対策として「Shift キーを押し続けることで自動実行マクロを無効にする」という方法があるが、これも正しく働かないため、事前にウイルスチェックを行うことが必要である。

Palm に転送された qsh ファイルは、そのデータ部分のみのファイルとなり、この場合はわずか 23 バイトであった。これを Palm 上で動作する Quicksheet で開いても、当然 Laroux ウィルスの活動は起こらなかった。なお、Quicksheet はマクロの表示・編集・実行機能を提供しておらず(図 4)、現在の Quicksheet 自体にはマクロウイルスの危険性はないと言える。

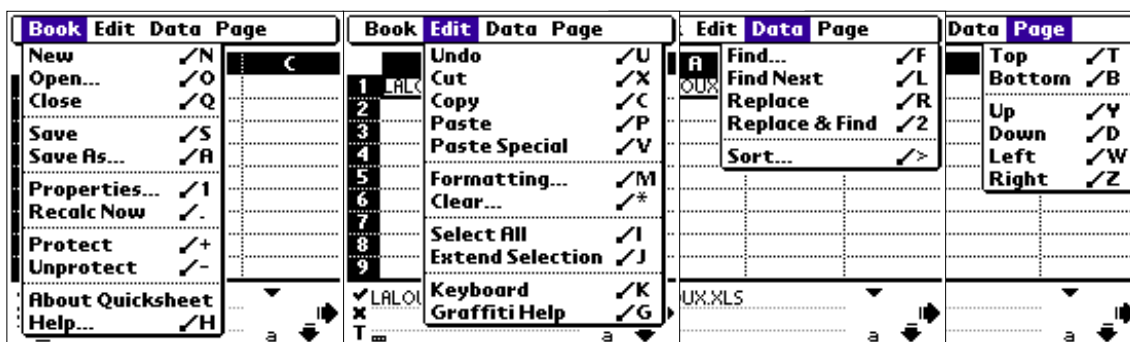


図4: Quicksheet のメニュー

<sup>4</sup> Excel データファイル中のすべてのワークシートが空の場合は変換エラーが発生する。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先の元ファイルの内容が更新され、マクロを含まない xls ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Laroux (64B)      PC: Laroux.qsh (2.1KB)  
 PC: Laroux.qsh (2.1KB)      PC: Laroux.xls (13.5KB)

#### SheetToGo -----

SheetToGo の場合も、PC 側でファイルを Palm 側アプリケーションのデータ形式に変換してから転送を行う。

PC: Laroux.xls (17.5KB)      PC: Laroux.pdb (1.2KB)  
 PC: Laroux.pdb (1.2KB)      Palm: Laroux (1.2KB)

ファイルの内容が SheetToGo 用の pdb ファイルに変換され、拡張子が"pdb"となり、ファイルサイズが大幅に減少した。変換後の pdb ファイルは、PalmOS アプリケーションのデータ用の形式<sup>5</sup>になっており、バイナリエディタで開いて内容を視認した結果、マクロコードは存在しなかった。

転送したファイルを Palm 上の SheetToGo で開いても、**Laroux ウイルスの活動は起こらなかった**。なお、SheetToGo はマクロの表示・編集・実行機能を提供しておらず(図 5)、現在の SheetToGo にはマクロウイルスの危険性はないと言える。

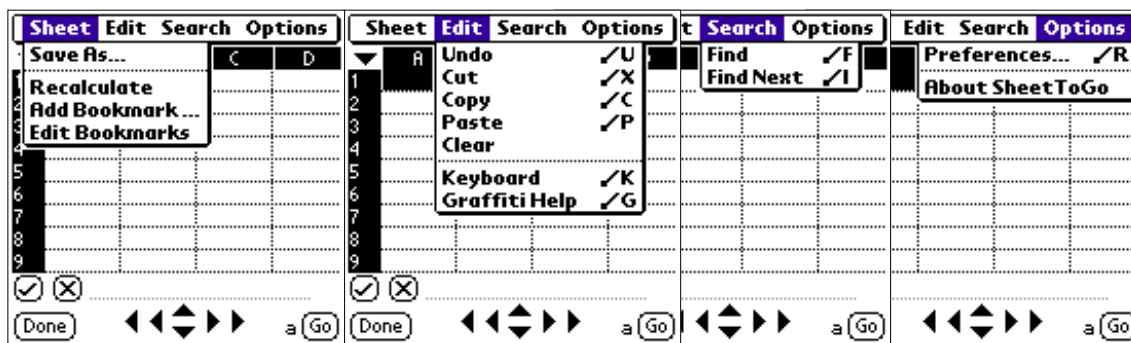


図5: SheetToGo のメニュー

また、Palm 上で編集したファイルを PC へ戻すと、リンク先の元ファイルの内容が更新され、マクロを含まない xls ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Laroux (1.3KB)      PC: Laroux.pdb (1.3KB)

<sup>5</sup> PDB ファイルは Palm データベース形式のファイル。

### 3.1.2 メールへの添付(HotSync による送受信)

次に、電子メールにウイルスファイルを添付した場合の実験を行う。

Palm の標準メールアプリケーションで電子メールを送受信する場合は、メールを HotSync で転送し、実際の送受信は PC 側で行う。

ファイルを添付したメールを HotSync 経由で受信しても、添付ファイルが含まれていたことを示すメッセージが表示されるだけで(図 6)、ファイル本体は含まれていなかった。これは、Palm の標準メールアプリケーションが最大 8K バイトのメールしか受信できず、添付ファイルにも対応していないためであり、**現状の標準メールアプリケーションでは添付ファイルを利用したウイルスの拡散はあり得ない**ということを示している。

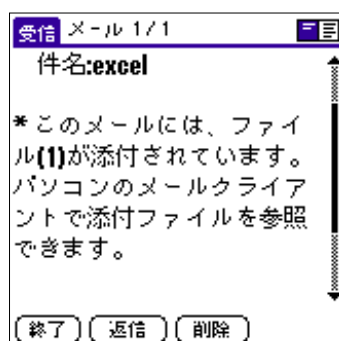


図6: 添付ファイルがあったことを示すメッセージ

以降、この実験は意味を持たないため省略する。

### 3.1.3 メールへの添付(直接送受信)

PalmOS マシンのために、携帯電話や PHS を利用して電子メールを送受信できるアプリケーションソフトウェアが公開されている。これは PalmOS の標準アプリケーションではないが、PalmOS マシンに付属していることが多い。今回は携帯電話と Palm 社製の MultiMail Professional を使用した。

ファイルを添付したメールを MultiMail で受信しても、添付ファイルがあったことを示すメッセージ「--- Attachment Laroux.xls---」が本文末尾に表示されるだけで、ファイル本体は含まれていなかった。これは MultiMail が最大 60K バイトのメールしか受信できず、添付ファイルに対応していないためであり、**現状の MultiMail では添付ファイルを利用したウイルスの拡散はあり得ない**ということを示している。

以降、この実験も意味を持たないため省略する。

## 3.2 W97M/X97M/P97M/Tristate

Tristate は Microsoft Word、Microsoft Excel および Microsoft PowerPoint 間で感染動作することが可能なマクロウイルスである。ここでは、Tristate ウイルスに感染している Excel ファイル "Tristate.xls" を検体とし、Excel データを扱うことのできる Quicksheet と SheetToGo で開いたときの動作を調査する。

### 3.2.1 ファイル転送

Quicksheet -----

ファイルサイズ以外は前述した Laroux ウイルスと同じ結果となった。

PC 側の Quickoffice Desktop でファイル形式を変換し、HotSync で PC と Palm との間でファイル転送を行った。

PC: Tristate.xls (102KB)	PC: Tristate.qsh (49.3KB)
PC: Tristate.qsh (49.3KB)	Palm: Tristate (45.9KB)

PC 上でのファイル形式の変換の時点で拡張子が "qsh" となり、ファイルサイズが半減した。変換後の qsh ファイルにはマクロコードは存在しなかった。ただし、ファイル形式の変換の際に PC が感染する恐れがあるため、事前にウイルスチェックを行っておく必要がある。

転送したファイルを Quicksheet で開いても、Tristate ウイルスの活動は起こらなかった。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない xls ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Tristate (33.0KB)	PC: Tristate.qsh (35.8KB)
PC: Tristate.qsh (35.8KB)	PC: Tristate.xls (37.5KB)

SheetToGo -----

SheetToGo の場合も、PC 側でファイルを Palm 側アプリケーションのデータ形式に変換してから転送を行う。しかしながら、ファイル変換の際に pdb ファイルが 0 バイトとなってしまった。

PC: Tristate.xls (102KB)	PC: Tristate.pdb (0B)
PC: Tristate.pdb (0B)	Palm: Tristate (不明)

当然ながら、転送したファイルを Quicksheet で開こうとしても中身がないため開くことはできず、もちろん Tristate ウイルスの活動は起こらなかった。

この、ファイルサイズが 0 になる現象は、おそらく検体 xls ファイルのバージョン等によ

って起きる問題であり、Tristate ウイルスのマクロが原因ではないだろう。ちなみに、先述の Laroux.xls は Excel 95 で作成されたファイルであり、Tristate.xls は Excel 97/2000 のファイルである。確認のため、独自に Excel 97/2000 で作成した xls ファイルを変換しようとするとうエラーが発生し変換できなかったが(図 7)、Excel 95 の xls ファイルは問題なく変換できた。これはやはり SheetToGo のファイル変換機能の問題であろう。

仮にこの問題が無く、変換が成功していたとしても、マクロは pdb ファイル内には残らず、Palm 上では安全であることは間違いない。

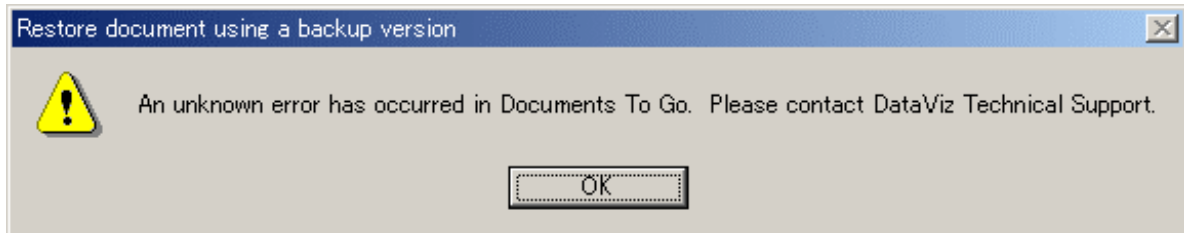


図7: Documents To Go の変換エラー

### 3.3 W97M/Class

Class は Microsoft Word で動作するマクロウイルスである。ここでは、Class ウイルスに感染している "Class.doc" を検体とし、Word 文書を扱うことのできる Quickword と WordToGo で開いたときの動作を確認する。

#### 3.3.1 ファイル転送

Quickword -----

PC 側の Quickoffice Desktop でファイル形式を変換し、HotSync で PC と Palm との間でファイル転送を行った。

PC: Class.doc (315KB)    PC: Class.qwd (6.3KB)  
PC: Class.qwd (6.3KB)    Palm: Class (3.4KB)

PC 上でのファイル形式の変換の時点で拡張子が "qwd" となり、ファイルサイズが激減した。変換後の qwd ファイルはテキストファイルであり、元の doc ファイルへのリンク情報と文書ファイルのテキスト部分が格納されていたが、マクロコードは存在しなかった。

ただし、ファイル形式の変換の際、バックグラウンドで Word が起動して対象ファイルが読み込まれ、そのファイルデータを基に qwd 形式のファイルが生成されるのだが、この時点で自動実行ウイルスマクロが動作し PC が感染してしまう。これは Word のセキュリティレベルに関係なく実行されるため注意が必要である。なお、前述の Excel の場合とは異なり、Word でファイルを開くときのウイルス対策として「Shift キーを押し続けることで自動実行マクロを無効にできる」という方法は有効である<sup>6</sup>。しかしながら、やはり事前にウイルスチェックを行うことが望ましい。

Palm に転送された qwd ファイルは、そのデータ部分のみのファイルとなり、この場合は 3.4KB であった。これを Palm 上で動作する Quickword で開いても、Class ウイルスの活動は起こらなかった。なお、Quickword はマクロの表示・編集・実行機能を提供しておらず(図 8)、現在の Quickword にはマクロウイルスの危険性はないと言える。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先の元ファイルの内容が更新され、マクロを含まない doc ファイルになった<sup>7</sup>。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Class (5.6KB)    PC: Class.qwd (7.8KB)  
PC: Class.qwd (7.8KB)    PC: Class.doc (67.0KB)

---

<sup>6</sup> この Excel と Word の挙動の違いは、将来のバージョンアップやアップデートパッチにより改善されることが期待される。

<sup>7</sup> ただし、罫線は消え、文書末にゴミデータが付加されていた。

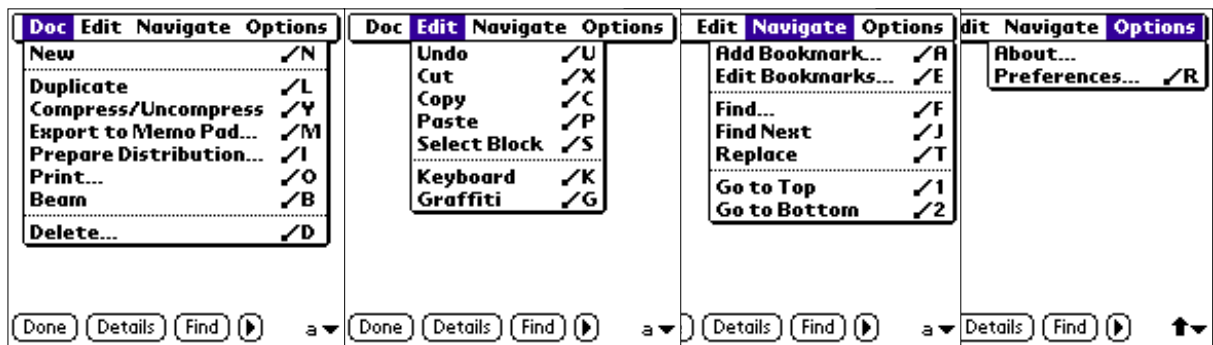


図8: Quickword のメニュー

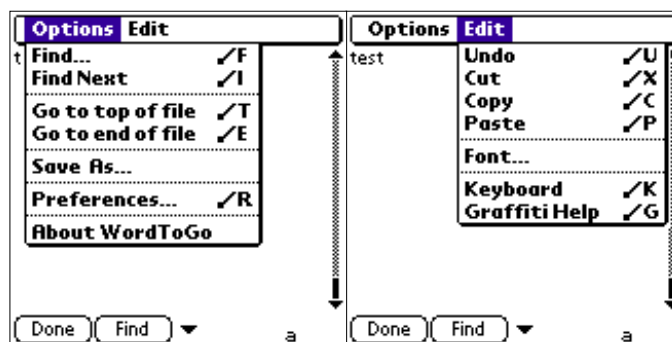
## WordToGo

WordToGo の場合も、PC 側でファイルを Palm 側アプリケーションのデータ形式に変換してから転送を行う。

PC: Class.doc (63.5KB<sup>8</sup>)      PC: Class.pdb (2.4KB)  
 PC: Class.pdb (2.4KB)      Palm: Class (2.4KB)

ファイルの内容が WordToGo 用の pdb ファイルに変換され、拡張子が"pdb"となり、ファイルサイズが減少した。変換後の pdb ファイルは、PalmOS アプリケーションのデータ用の形式になっており、バイナリエディタで開いて内容を視認した結果、マクロコードは存在しなかった。

転送したファイルを Palm 上の WordToGo で開いても、**Class ウイルスの活動は起こらなかった**<sup>9</sup>。なお、WordToGo はマクロの表示・編集・実行機能を提供しておらず(図 9)、現在の WordToGo ではマクロウイルスの危険性はないと言える。



<sup>8</sup> 元の検体ファイル(315KB)の場合、変換中にプログラムが停止してしまった。ここでは文書データの大半を削除した小さな感染ファイルで実験している。

<sup>9</sup> ただし、日本語文はすべて文字化けしていた。

図9: WordToGo のメニュー

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない doc ファイルになった。ただし、pdb ファイルへの変換の際に日本語文はすべて文字化けしており、そのまま PC へ転送した場合は文字化けした状態の doc ファイルになってしまう。これは WordToGo が日本語に対応していないことが原因であろう。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Class (2.4KB)	PC: Class.pdb (2.4KB)
PC: Class.pdb (2.4KB)	PC: Class.doc (15KB)



### 3.4 W97M/Marker

Marker は Microsoft Word で動作するマクロウイルスである。ここでは、Marker ウィルスに感染している "Marker.doc" を検体とし、Word 文書を扱うことのできる Quickword と WordToGo で開いたときの動作を確認する。

#### 3.4.1 ファイル転送

Quickword -----

ファイルサイズ以外は前述した Class ウィルスと同じ結果となった。

PC 側の Quickoffice Desktop でファイル形式を変換し、HotSync で PC と Palm との間でファイル転送を行った。

PC: Marker.doc (42.5KB)	PC: Marker.qwd (145B)
PC: Marker.qwd (145B)	Palm: Marker (30B)

PC 上でのファイル形式の変換の時点で拡張子が "qwd" となり、ファイルサイズが激減した。これは検体ファイルの本文のサイズがわずか十数文字<sup>10</sup>であったためであろう。やはり、変換後の qwd ファイルにはマクロコードは存在しなかった。ただし、ファイル形式の変換の際に PC が感染する恐れがあるため、事前にウイルスチェックを行っておく必要がある。

転送したファイルを Quickword で開いても、Marker ウィルスの活動は起こらなかった。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない doc ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Marker (31B)	PC: Marker.qwd (152B)
PC: Marker.qwd (152B)	PC: Marker.doc (19.0KB)

WordToGo -----

ファイルサイズ以外は前述した Class ウィルスと同じ結果となった。

WordToGo の場合も、PC 側でファイルを Palm 側アプリケーションのデータ形式に変換してから転送を行う。

PC: Marker.doc (42.5KB)	PC: Marker.pdb (398B)
PC: Marker.pdb (398B)	Palm: Marker (168B)

---

<sup>10</sup> 検体ファイルの文章データは「Marker.doc」と空行の2行のみであり、改行コードを含めても14バイトしかない。ただし、変換後のpdbファイルには文章データ以外にPalmOS用ファイルとしての構造情報を含んでいる。

ファイルの内容が WordToGo 用の pdb ファイルに変換され、拡張子が"pdb"となり、ファイルサイズが激減した。変換後の pdb ファイルは、PalmOS アプリケーションのデータ用の形式になっており、バイナリエディタで開いて内容を視認した結果、マクロコードは存在しなかった。

転送したファイルを WordToGo で開いても、**Marker ウイルスの活動は起こらなかった。**

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない doc ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Marker (175B)	PC: Marker.pdb (405B)
PC: Marker.pdb (405B)	PC: Marker.doc (14.0KB)

### 3.5 W97M/Ethan

Ethan は Microsoft Word で動作するマクロウイルスである。ここでは、Ethan ウイルスに感染している "Ethan.doc" を検体とし、Word 文書を扱うことのできる Quickword と WordToGo で開いたときの動作を確認する。

#### 3.5.1 ファイル転送

パームサイズ PC -----

ファイルサイズ以外は前述した Class ウイルスと同じ結果となった。

PC 側の Quickoffice Desktop でファイル形式を変換し、HotSync で PC と Palm との間でファイル転送を行った。

PC: Ethan.doc (37.0KB)	PC: Ethan.qwd (135B)
PC: Ethan.qwd (135B)	Palm: Ethan (23B)

PC 上でのファイル形式の変換の時点で拡張子が "qwd" となり、ファイルサイズが激減<sup>11</sup>した。変換後の qwd ファイルにはマクロコードは存在しなかった。ただし、ファイル形式の変換の際に PC が感染する恐れがあるため、事前にウイルスチェックを行っておく必要がある。

転送したファイルを Quickword で開いても、Ethan ウイルスの活動は起こらなかった。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない doc ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Ethan (24B)	PC: Ethan.qwd (139B)
PC: Ethan.qwd (139B)	PC: Ethan.doc (19.0KB)

WordToGo -----

ファイルサイズ以外は前述した Class ウイルスと同じ結果となった。

WordToGo の場合も、PC 側でファイルを Palm 側アプリケーションのデータ形式に変換してから転送を行う。

PC: Ethan.doc (37.0KB)	PC: Ethan.pdb (387B)
PC: Ethan.pdb (387B)	Palm: Ethan (157B)

ファイルの内容が WordToGo 用の pdb ファイルに変換され、拡張子が "pdb" となり、ファイルサイズが激減した。変換後の pdb ファイルは、PalmOS アプリケーションのデータ用の

---

<sup>11</sup> 検体ファイルの文章データは「test」の1行のみで、改行を含めても6バイトしかなかったため。

形式になっており、バイナリエディタで開いて内容を視認した結果、マクロコードは存在しなかった。

転送したファイルを WordToGo で開いても、Ethan ウイルスの活動は起こらなかった。

また、Palm 上で編集したファイルを PC へ戻すと、リンク先である元のファイルの内容が更新され、マクロを含まない doc ファイルになった。Palm 上でファイルを更新しなかった場合は、HotSync を実行しても PC 上のリンク先ファイルは変化しない。

Palm: Ethan (174B)	PC: Ethan.pdb (404B)
PC: Ethan.pdb (404B)	PC: Ethan.doc (14.0KB)

## 4 実験結果の考察

ここでは、以上の実験結果をまとめ、PalmOS 環境におけるマクロウイルスの動作に関する考察を行う。

## 4.1 PalmOS 用アプリケーションソフトの機能について

PalmOS マシンには、それが小型軽量性を重視しているためか、Microsoft Office 系の文書ファイルを扱うことのできるアプリケーションは標準では入っておらず、直接扱うことはできなかった。

PalmOS では、市販の Quickoffice や Documents To Go のようなアプリケーションをインストールすることで、Office 系のファイルを扱うことができるようになる。しかしながら、これらは独自形式のファイルを読み書きする。それらの形式のファイルにはマクロは含まれていなかった。また、どちらのアプリケーションにもマクロを作成・実行するための機能が付いていなかった。したがって、Quickoffice や Documents To Go はマクロに対応しておらず、マクロウイルスが動作することはあり得ない。

しかしながら、もしこれらのアプリケーションがバージョンアップなどでマクロを解釈・実行できるようになったり、マクロを解釈・実行できる PalmOS アプリケーションが開発・販売されたりした場合は、PalmOS がマクロウイルスに感染することは十分考えられる。現在の PalmOS マシンではアプリケーションは RAM にインストールされ、現行マシンの RAM サイズが多くても 8MB であることを考えると、ROM や RAM の容量の問題によってマクロがサポートされることはすぐには実現しそうにないが、将来、大容量の ROM や RAM が PalmOS マシンに搭載されるようになれば、この懸念は現実のものとなる可能性があるだろう。

## 4.2 ファイル変換について

Quickoffice や Documents To Go にはマクロ機能がないため、PC の Office 系ファイルはマクロのない形式に変換される。この変換によっていったん削除されたマクロは、PC 側に戻すときの逆変換によっても復活することはない。したがって、PC ユーザから Office 系ファイルを受け取る Palm ユーザも、PalmOS マシン上で作成・編集したファイルを受け取る PC ユーザも、マクロウイルスの心配は少ない。

ただし、PC 上の Quickoffice Desktop でファイル形式を変換する際、バックグラウンドで Office アプリケーションが起動して自動実行マクロが実行されてしまうため、マクロウイルスに感染したファイルを変換すると PC が感染してしまうことになる。通常は、Office アプリケーションのセキュリティレベルを「高」に設定しておけば、デジタル署名のないマクロは実行されないのだが、Quickoffice のファイル変換ではセキュリティレベルにかかわらず実行されてしまうため、あらかじめウイルス検査を行う必要がある。Documents To Go ではこの問題は発生しない。

なお、PC 上の Office 系ファイルを変換せずに Palm に転送することはできない。

### 4.3 メール添付について

PalmOS マシンと PC の間でのメール送受信は、ケーブル接続によるファイル転送と携帯電話等による直接送受信が考えられるが、どちらも Palm 側のメールアプリケーションの機能により添付ファイルは無視され、添付ファイルで拡散するウイルスの問題が Palm 上で発生することはない。

例えば、ウイルスが添付された電子メールを受け取った場合、PC 側でさえ添付ファイルを開かなければ安全である。PC で受信して Palm に転送しても、Palm で直接受信しても、メール本文は問題なく読むことができ、そのメールに返信したり第三者に転送したりしても、添付ファイルは含まれないため問題は生じない。



## 5 まとめ

携帯端末の普及により、PalmOS マシンがインターネット環境でも広く利用されるようになれば、Palm ユーザが Windows 95/98 等で問題となっているマクロウイルスに遭遇する場合も増えてくると考えられる。

本報告書では、Palm 社の PalmOS を搭載している携帯端末でのマクロウイルスの動作を実験によって確認し、現状では PalmOS マシン自体に危険が及ぶことはなく、また、ウイルスファイルをそのまま別の電子メールユーザに転送してしまう恐れもないと結論づけた。しかしながら、アプリケーションによっては PC 側のファイル変換の際にウイルスに感染する恐れがあるため、Office 系ファイルを扱う場合は事前に PC 側で検査することが重要である。

また、今後、Microsoft Office シリーズのマクロを解釈し実行できる PalmOS 用アプリケーションが出現したら、その環境の危険性は Windows 95/98 等と何ら変わらなくなるだろう。

この結果は、PalmOS マシンに被害がないとはいえ、PC 側で十分注意しなければならないことを示し、また、PalmOS 用 Office アプリケーションの今後の機能拡張に警鐘を鳴らすものである。