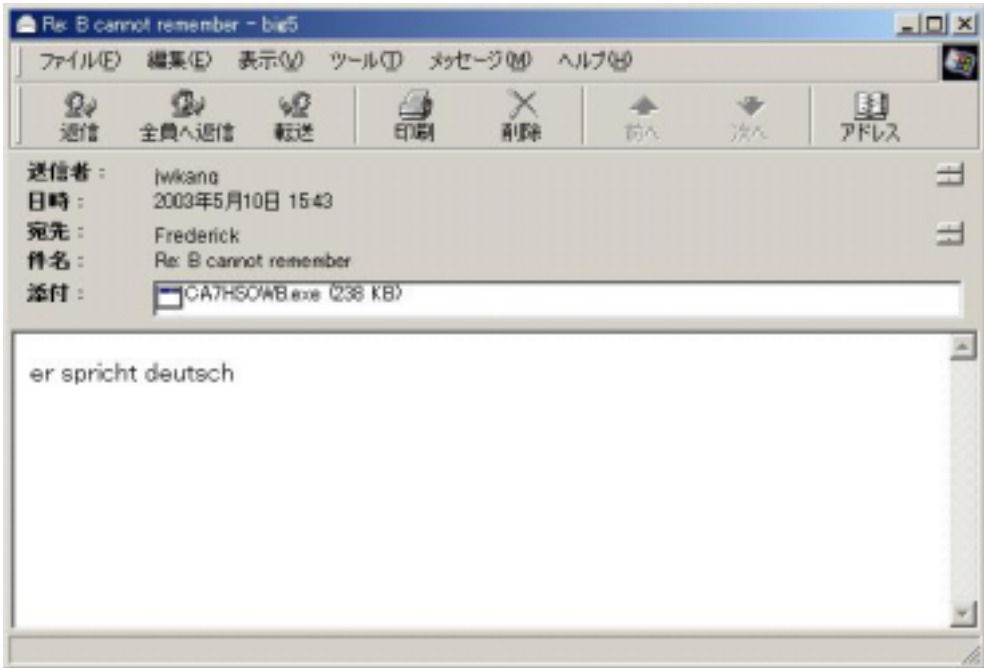


## ウイルス解析報告書

<b>ウイルス名</b>	W32.HLLW.Fizzer@mm (別名: W32/Fizzer@mm[McAfee], Win32.Fizzer[CA], W32/Fizzer-A [Sophos], WORM_FIZZER.A[Trend], Fizzer[F-Secure], Win32/Fizzer.A@mm[RAV], I-Worm.Fizzer[KAV])
<b>プログラム名及び容量(添付ファイル名)</b>	プログラム名 : iservc.exe, initbak.dat (感染コンピュータにコピーされるワームの実体) 容 量 : 241,664 バイト 添付ファイル名 : ファイル名はランダムに生成され、exe、pif、com、scr のいずれかの拡張子が付けられる。
<b>種 別</b>	ワーム
<b>プログラム言語</b>	不明
<b>発 症 環 境</b>	Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me
<b>発 見 日 時</b>	2003 年 5 月 9 日
<b>発見場所(発信地)</b>	ドイツ(最初に感染報告があった場所)
<b>危 険 性</b>	感染力が強く、バックドア機能を有しており危険である。危険度は 5 段階の 3
<b>発 症 条 件</b>	主にワームが添付されたメールの添付ファイルを開いたときに発症する。
<b>ウイルスの活動影響</b>	<ul style="list-style-type: none"> <li>・ ワーム自身を電子メールに添付し、Windows のアドレス帳に登録されている連絡先全員に送信する。</li> <li>・ mIRC を使ってリモートの攻撃者と通信するなどのバックドア機能を備えている。</li> <li>・ キーストロークのログを生成し保存する。</li> <li>・ KaZaA ファイル共有ネットワークを介しても感染拡大する。</li> <li>・ 様々なウイルス対策プログラムのプロセスを停止させる。</li> </ul>
<b>被 害 規 模</b>	大規模
<b>変種、亜種の有無</b>	無
<b>ウイルスの動作概要</b>	<p>ワームによって送信されるメールには次の特徴がある。</p>  <p><b>件名:</b> ワームが保有しているリストから以下のような文をランダムに選択する。(文頭に Re:または Fw: がつく場合がある)</p> <ul style="list-style-type: none"> <li>・ I thought this was interesting...</li> <li>・ rather psychedelic...</li> </ul>

- found this on the net, you might like it...
- discotheque
- imbrue
- Damn it feels good to be gangsta.
- The way I feel - Remy Shand
- Paradigm Shift
- WASSUP!
- Know Thyself
- Hell
- I love you
- Please discard if you don't like or agree with our present leadership...
- little popup remover
- B cannot remember
- Yo, WASSUP, B?
- an interesting program...
- You might not appreciate this...
- I think you might find this amusing...
- LOL
- check this out... hehehe
- question...
- see you tomorrow.
- how are you?
- you need to lose weight.
- why?
- kind of simple, but fun nonetheless.
- check it out. 等

**本文:** ワームが保有しているリストから以下のような文をランダムに選択する。

- I sent this program (Sparky) from anonymous places on the net.
- The way to gain a good reputation is to endeavor to be what you desire to appear.
- There is only one good, knowledge, and one evil, ignorance.
- Watchin' the game, having a bud.
- Did you ever stop to think that viruses are good for the economy? Maybe the primary creators of the world's worst viruses are the companies that make the Anti-Virus software.
- Today is a good day to die...
- so, how are you?
- the attachment is only for you to look at
- you must not show this to anyone...
- delete this as soon as you look at it...
- Let me know what you think of this...
- If you don't like it, just delete it.
- thought I'd let you know
- you don't have to if you don't want to. 等

**添付ファイル:** 添付ファイル名はランダムに生成され、以下のいずれかの拡張子が選択される。

- exe
- pif
- com
- scr

**ワームが実行されると次のような動作を行う。**

1. Windows のインストール先フォルダ (標準では C:\Windows または C:\WINNT) に次のファイルを作成する。
  - ・ iservc.exe (ワームの実体)
  - ・ initbak.dat (ワームの実体)
  - ・ ProgOp.exe (ワームコンポーネントの1つ)
  - ・ iservc.dll (ワームのコンポーネントの1つ。キーストロークログを記録する。)
  - ・ data1-2.cab (ワームが感染先のコンピュータ上で発見したメールアドレスを暗号化して記録する)
  - ・ iservc.dat (ワームコンポーネントの1つ)
  - ・ Uninstall.pky (ワームコンポーネントの1つ)
  - ・ upd.bin (ワームコンポーネントの1つ)
2. Windows の起動時に必ずワームが実行されるようにするために、レジストリを操作する
  - ・ 対象レジストリキー  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - ・ 追加する値  
"SystemInit" = "%iservc.exe"システム起動時に、「iservc.exe」をプロセスとして起動する。
3. テキストファイルを開くとワームが実行されるようにするために、レジストリを操作する。
  - ・ 対象レジストリキー  
HKEY\_LOCAL\_MACHINE\Software\CLASSES\txtfile\shell\open\command
  - ・ 変更する値  
@ = "%ProgOp.exe 0 7 %notepad.exe %1"%initbak.dat"iservc.exe'
4. 「SparkyMutex」というミューテックを作成し、ワームが1度に1つのみ実行されるようにする。
5. Windows のアドレス帳、cookies、インターネットのテンポラリファイル、現在のユーザの個人用フォルダに保存されているファイルからメールアドレスを収集する。  
その後、収集した全てのメールアドレスに対し、そのコンピュータ上で現在使用されている MAPI 対応プログラムを使用して自分自身を送信する。  
このワームは差出人の名前とメールアドレスを詐称する可能性がある。
6. 次のいずれかの文字列を含むプロセス名を、全て停止させようとする。
  - ・ NAV
  - ・ SCAN
  - ・ AVP
  - ・ TASKM
  - ・ VIRUS
  - ・ F-PROT
  - ・ VSHW
  - ・ ANTIV
  - ・ VSS
  - ・ NMAIN
7. ワームが保有する様々なユーザ名を使用して、様々な IRC サーバへの接続を試みる。接続後は、

他の攻撃者から送信されるメッセージを待ち受ける。なお、ワームが接続を試みる IRC サーバ例は次のとおりである。

- ・ irc.accessirc.net
- ・ irc.aceirc.net
- ・ irc.ablenet.org
- ・ irc.abovenet.org
- ・ irc.afternet.org
- ・ irc.all-defiant.org
- ・ irc.allochat.net
- ・ irc.alphanine.net
- ・ irc.altnet.org
- ・ irc.amcool.net
- ・ irc.amiganet.org
- ・ irc.angeleyez.net
- ・ irc.aniverse.com
- ・ irc.another.net
- ・ irc.arabchat.org
- ・ irc.arabmirc.net
- ・ irc.astrolink.org
- ・ irc.asylum-net.org
- ・ irc.auiirc.net
- ・ irc.aurosoniq.net
- ・ irc.auscape.org
- ・ irc.aussiechat.org
- ・ irc.awesomechat.net
- ・ irc.awesomechristians.com
- ・ irc.axenet.org
- ・ irc.aXpi.net
- ・ irc.ayna.org
- ・ irc.azzurra.org
- ・ irc.bahamutirc.net
- ・ irc.bappy.eu.org
- ・ irc bdsm-net.com
- ・ irc.beyondirc.net
- ・ irc.dal.net
- ・ irc.eu.dal.net

8 . 全てのキーストローク記録を、「iservc.klg」という暗号化ファイルとして保存する。保存場所は Windows のインストール先フォルダ (標準では C:\Windows または C:\WINNT) である。

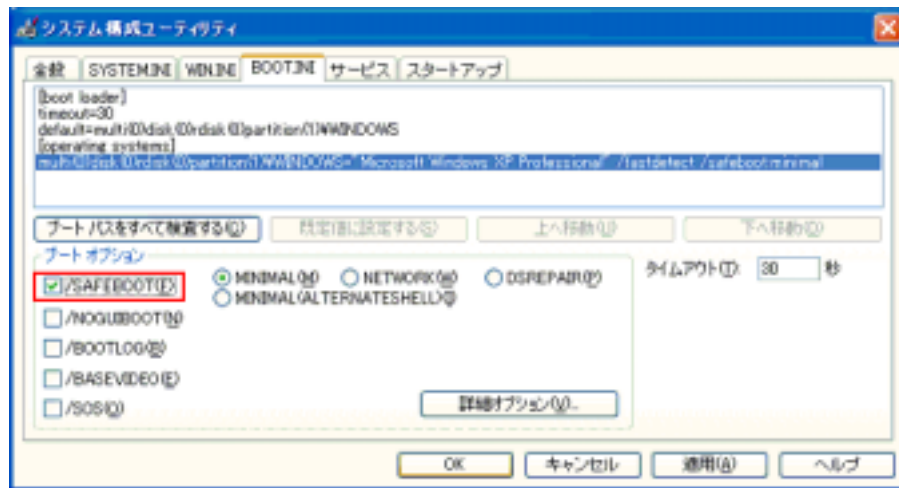
9 . KaZaA ファイル共有ネットワークを介して感染を拡大するために、自分自身を KaZaA ファイルのダウンロード用ディレクトリにランダムなファイル名でコピーする。

10 . AOL Instant Messenger (AIM) のチャットルームに、新規に作成したランダムな名前のユーザとして接続し、ハッカーからの指示を待機する。

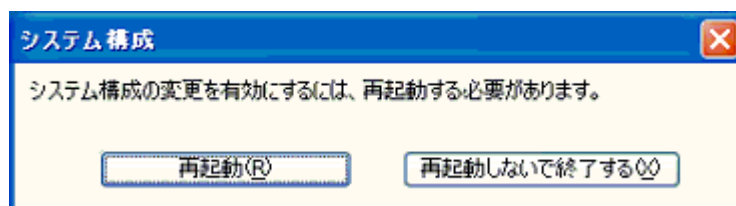
11 . ポート 81 で HTTP サーバとして動作する。

12 . バックドア用の通信ポートとして、以下のポートを使用する。

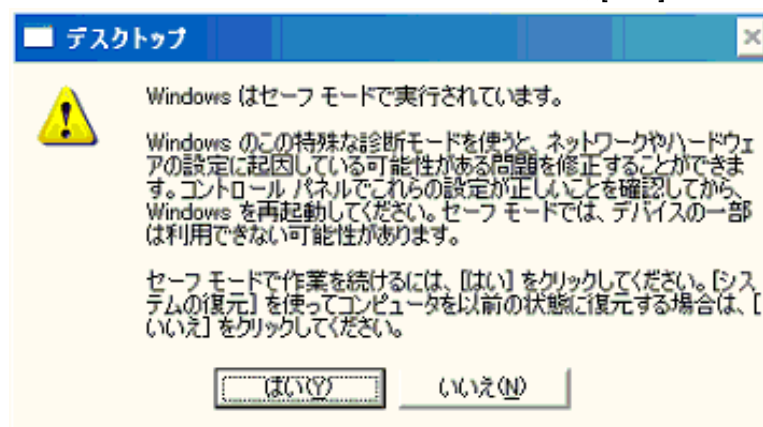
	<ul style="list-style-type: none"> <li>・ TCP/2018 (コマンド送受信)</li> <li>・ TCP/2019 (ファイル送受信)</li> <li>・ TCP/2020 (コンソール用)</li> <li>・ TCP/2021 (画面キャプチャ送信用)</li> </ul> <p>13. 特定のサイトに接続し、自分自身のアップデートを入手しようとする。ただし、そのサイトは現在利用できなくなっている。</p>
<b>感染・発症防止方法</b>	<p>1. 「ウイルスの動作概要」に記述した内容のメールが届いた場合には、安易にメールを開封しない。</p> <p>2. 特に拡張子(.exe、.pif、.com、.scr)が付いたメールの添付ファイルは安易に開封しない。</p> <p>3. 予期せぬメールが届いた場合には、安易にメールを開封しない。</p>
<b>ウイルスの駆除方法</b>	<p><b>手動による修復を行う場合、コンピュータに関する高度な知識を必要するため、誤って操作するとコンピュータが正常に動作しなくなる場合があります。</b></p> <ol style="list-style-type: none"> <li>1. 被害拡大防止のため、接続されているネットワークから切り離す。</li> <li>2. コンピュータをセーフモードで再起動する       <ol style="list-style-type: none"> <li>(1) <b>Windows XP をセーフモードで起動する方法</b></li> </ol> <p>Windows XP は、セーフモードでシステムを起動するためにいくつかの手順が用意されてる。コンピュータが起動可能な状態の場合は、1 番目のシステム構成ユーティリティを使用する手順を実行する事を推奨する。システムが起動しない状態であったり、最初の手順で起動に失敗する場合は、その後の手順を実行してシステムをセーフモードで起動することができる。</p> <p style="text-align: center;"><b>システム構成ユーティリティを使用して Windows XP をセーフモードで起動する方法 (推奨)</b></p> <p>Windows XP には、システム構成ユーティリティの機能が追加されている。Windows XP が通常に起動できる状態の場合は、この機能を使用する事で簡単にシステムをセーフモードで起動する事ができる。</p> <p>手順 1. 実行中のすべてのプログラムを停止する。</p> <p>手順 2. [スタート] ボタンをクリックし、[ファイル名を指定して実行] を選択する。</p> <p>手順 3. 以下のように名前ボックスに msconfig と入力し、[OK] ボタンをクリックする。</p> <div data-bbox="432 1413 1187 1742" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;"><b>ファイル名を指定して実行</b></p> <p>実行するプログラム名、または開くフォルダやドキュメント名、インターネットリソース名を入力してください。</p> <p>名前(O): <input type="text" value="msconfig"/></p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="キャンセル"/> <input type="button" value="参照(B)..."/> </p> </div> <p>手順 4. システム構成ユーティリティで [BOOT.INI] タブを選択し、[ブートオプション]の項目 [/SAFEBOOT] にチェックを入れ、[OK] ボタンをクリックする。</p> </li> </ol>



手順5. 以下のダイアログで [再起動] をクリックする。



しばらくすると、コンピュータがセーフモードで起動する。セーフモードの起動に成功すると、ログオン後に以下のような確認ダイアログが表示されるので、[はい]をクリックする。



**注意:** 再びノーマルモードで Windows XP を起動する場合は、同様の手順を行い、**手順 4** で [/SAFEBOOT] からチェックを解除する。

#### Windows XP をセーフモードで起動するその他の方法

**注意:** ご使用のコンピュータに複数のオペレーションシステムがインストールされており、マルチブート環境になっている場合は、**手順 3**の操作が異なる。

Windows XP では、セーフモードでソフトウェアのインストールはできない。

手順1. 以下のいずれかの操作を実行してシステムを起動させる。

#### Windows が起動中の場合:

- a. 実行中のすべてのプログラムを停止する。
- b. [スタート] ボタンをクリックし、[シャットダウン] を選択する。[Windows のシャットダウン]

ダイアログが表示される。

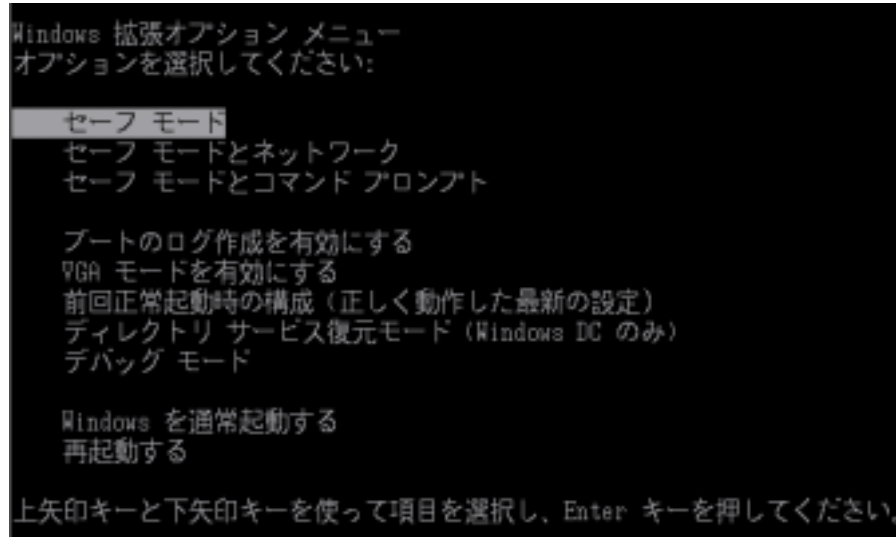
c. ドロップダウンリストで [再起動] を選択し、[OK] ボタンをクリックする。

・ **Windows が起動していない、または起動不能の場合:**

コンピュータの電源を入れ、システムを起動させる。

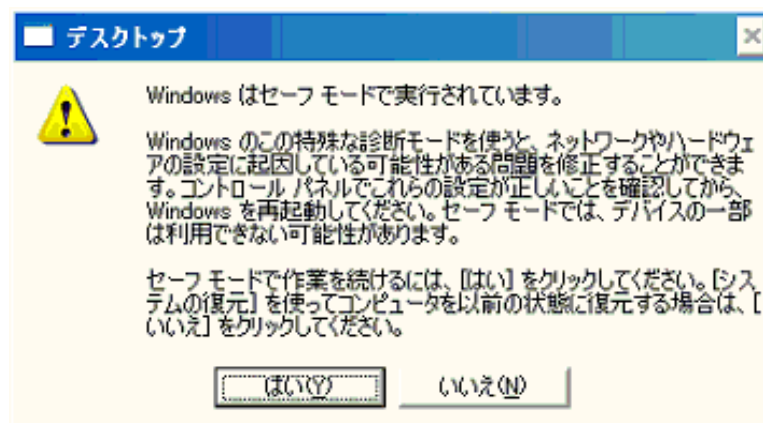
手順 2. システムの起動が始まり、コンピュータ製造元のロゴや BIOS の起動画面が表示される。

手順 3. 画面が真っ暗になってから Windows XP の起動ロゴが表示されるまでの間に、キーボードの [F8] キーを押す。Windows 拡張オプションメニューが表示される。



**注意:** マルチブート環境でご使用の場合は、Windows 起動ロゴの前に起動 OS の選択画面が表示される。この場合、Windows XP を選択して [Enter] キーを押した後に、すぐに [F8] キーを押す。コンピュータによっては、[F8] キーを何度も押すとキーボードエラーが発生する場合がある。この場合はコンピュータを再起動し、最初からやり直す。

手順 4. キーボードの [↑] [↓] キーでカーソルを移動して [セーフモード] を選択し、[Enter] キーを押す。しばらくすると、コンピュータがセーフモードで起動する。セーフモードの起動に成功すると、ログオン後に以下のような確認ダイアログが表示されるので、[はい] をクリックする。



(2) **Windows 2000 をセーフモードで起動する方法**

セーフモードは Windows の診断モードである。セーフモードで Windows 2000 を起動すると、システムの起動に必要な最小限のドライバ、サービスのみがロードされるため、インターネットやネットワークにアクセスできないなど、いくつかの機能が制限される。ビデオドライバには標準 VGA ドライバが使用されるため、解像度や色数が制限され、デスクトップやアプリケーションのインターフェイスが普段とは違った表示がされる。また、デスクトップ上のアイコンの位置が解像度に合わせて整列されて表示される。

手順 1. 以下のいずれかの操作を実行してシステムを起動させる。

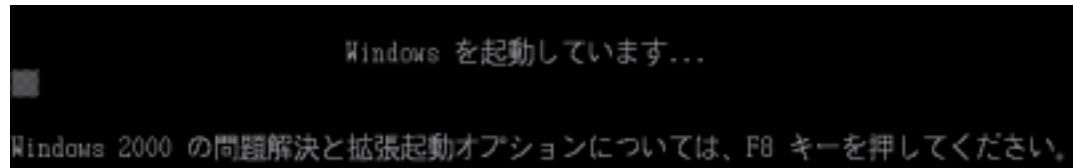
・ **Windows が起動中の場合:**

- 実行中のすべてのプログラムを停止する。
- [スタート] ボタンをクリックし、[シャットダウン] を選択する。[Windows のシャットダウン] ダイアログが表示される。
- ドロップダウンリストで [再起動] を選択し、[OK] ボタンをクリックする。

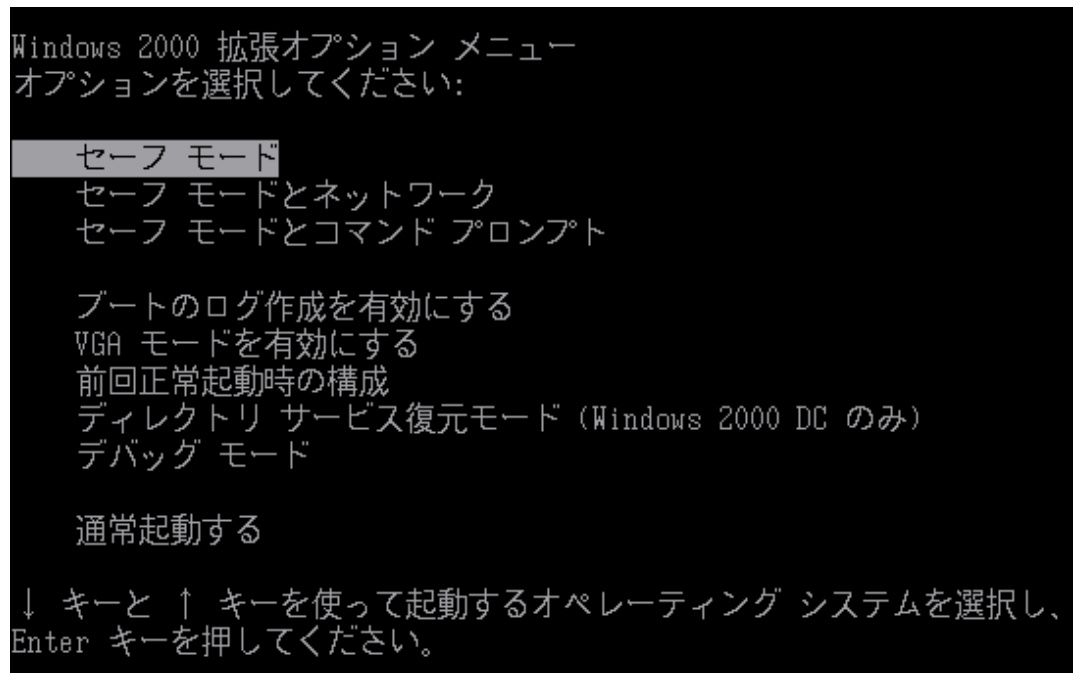
・ **Windows が起動していない、または起動不能の場合:**

コンピュータの電源を入れ、システムを起動させる。

手順 2. 真っ暗な画面が表示された後、「Windows を起動しています…」というメッセージが表示される。Windows 2000 の問題解決と拡張起動オプションについては…」というメッセージが表示されている間に、キーボードの[F8]キーを押す。



手順 3. Windows 2000 拡張オプションメニューで、キーボードの[↑][↓]キーでカーソルを移動して [セーフモード]を選択する。



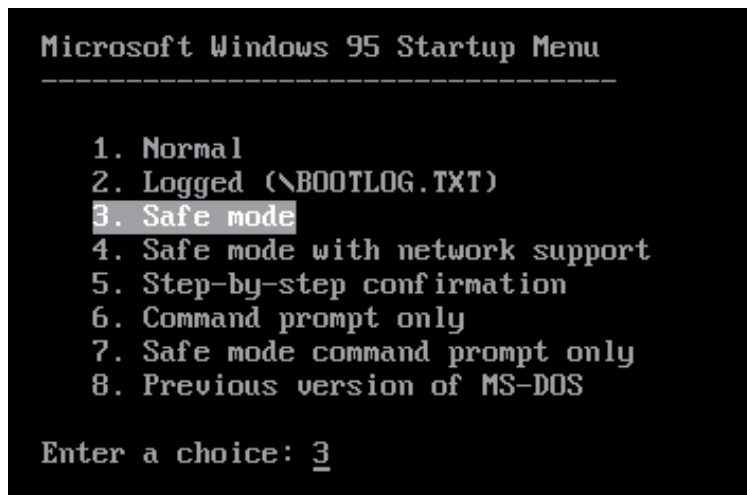
手順 4. [Enter]キーを押すと、しばらくして Windows 2000 がセーフモードで起動します。セーフモードの起動が成功すると、ログオン後に以下のような確認ダイアログが表示される。



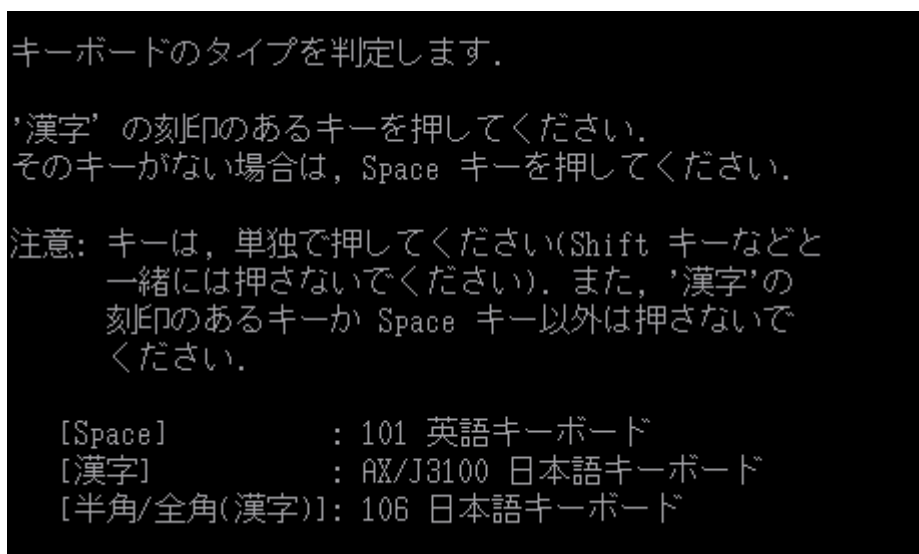
手順5. [OK]をクリックする。

(3) Windows 9x/Me をセーフモードで起動する方法

1. コンピュータを再起動する。
2. Windows の起動ロゴが表示される前の、「Windows 95 を起動しています」または「Starting Windows 95,」と表示されている画面で、キーボードの F8 キーを押す。
3. 起動メニューで、カーソルを移動して「Safe mode」を選択する。



4. キーボードの選択画面で[全角/半角]キーを押す。



5. デスクトップの 4 隅に「SAFE MODE」が表示され、セーフモードの確認ダイアログが表示される。



6. [OK]をクリックする。デスクトップアイコンが表示され、セーフモードでシステムが起動する。

**注意:** コンピュータによっては、出荷時に起動メニューを表示しないように設定されているものもある。何度[F8]キーを押しても起動メニューが表示されない場合は、[F8]キーではなく[F5]キーを押す。起動メニューがスキップされ、直接 Safe Mode が起動する。

### Windows 98/Me をセーフモードで起動する方法

Windows 98/Me では、トラブルシューティングのためにセーフモードで起動する方法がいくつか用意されている。コンピュータが起動不能になっている場合は**手順 1.**で、コンピュータが通常に起動する場合は**手順 1.**、**手順 2.**のいずれかの操作でシステムをセーフモードで起動する事ができる。

#### 手順 1: 直接セーフモードで起動する方法

1. コンピュータを再起動する。
2. 再起動が始まってから[Ctrl]キーを押し続ける。[Windows Startup Menu]が表示される。
3. カーソルを移動して「Safe mode」を選択する。
4. キーボードの選択画面で[全角/半角]キーを押す。
5. デスクトップの 4 隅に「SAFE MODE」が表示され、セーフモードの確認ダイアログが表示される。
6. [OK]をクリックする。デスクトップアイコンが表示され、セーフモードでシステムが起動する。

**注意:** コンピュータによっては、出荷時に起動メニューを表示しないように設定されているものもある。[Ctrl]キーを押しても[Windows Startup Menu]が表示されない場合は、[Ctrl]キーではなく[F5]キーを押す。起動メニューがスキップされ、直接セーフモードが起動する。

#### 手順 2: システム設定ユーティリティを使用してセーフモードで起動する方法

1. [スタート]ボタンをクリックし、[ファイル名を指定して実行]を選択する。
2. 名前ボックスに msconfig と入力し、[OK]ボタンをクリックする。
3. [詳細設定]ボタンをクリックする。[アドバンス トラブルシューティングの設定]ウィンドウが起動する。
4. スタートアップメニューを使用可能にする]にチェックを入れる。
5. [OK]ボタンをクリックしていき、すべてのウィンドウを閉じる。
6. コンピュータの再起動の確認ダイアログで、[はい]をクリックする。コンピュータが再起動し、[Windows Startup Menu]が表示される。
7. **手順 1. の操作 3.**以降の手順に従って、コンピュータを起動する。

**注意** Safe Mode の操作が完了後、同様に 1 から 4 の操作を実行し、[スタートアップメニューを使用可能にする]からチェックを外す。次回からコンピュータの起動時に[Windows Startup Menu]が表示されなくなる。

**以上のいずれの操作でもセーフモードで起動できなかった場合**

上記の操作を実行した時に Microsoft Windows Startup Menu が表示されず、[F5]キーを押してもセーフモードで起動できない場合は、以下の操作を実行する。

1. Windows 起動ディスクなどの、起動可能ディスクでない、通常のデータ用のフロッピーディスクをフロッピードライブに挿入する。
2. コンピュータを再起動する。

「Non-System Disk, please replace the disk and press any key. というようなエラーメッセージが表示されてから、フロッピーディスクを取り出す。

3. 「Microsoft Windows Startup Menu」の画面が表示されるまで、キーボードの[F8]キーを何度も押す。
4. カーソルを移動して「Safe mode」を選択する。

3. 操作されたレジストリを復元する。

1. [スタート]ボタンを押し、[ファイル名を指定して実行]をクリックする。( [ファイル名を指定して実行]ダイアログボックスが表示される。)
2. regedit と入力する。
3. その後、[OK]をクリックする(レジストリ エディタが開く)。
4. 次のレジストリキーを選択する。
  - ・ HKEY\_LOCAL\_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
5. 画面右側で次の値を削除する。
  - ・ "Systemlnit"="%windir%¥iservc.exe"
6. 次のレジストリキーを選択する。
  - ・ HKEY\_LOCAL\_MACHINE¥Software¥CLASSES¥txtfile¥shell¥open¥command
7. 画面右側で、標準値の設定を次の内容に変更する。
  - ・ notepad.exe %1
8. レジストリエディタを終了する。

4. Windows エクスプローラを開き、Windows フォルダにある次のファイルを検索して削除する。

- ・ iservc.exe
- ・ initbak.dat
- ・ ProgOp.exe
- ・ iservc.dll
- ・ data1-2.cab
- ・ iservc.dat
- ・ Uninstall.pky
- ・ Upd.bin

なお、無償修復ツールがウィルスワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。

その他

無