

明 細 書

セキュリティチェック機能を有する情報処理装置

技術分野

- 5 本発明は、実行すべきプログラムの真偽性をチェックするセキュリティチェック方法、更にこのセキュリティチェック機能を有する情報処理装置、この情報処理装置に使用されるビデオ信号制御回路及びプログラム格納装置に関する。

10

背景技術

- マイクロプロセッサの高速化に伴い、各種形態の情報処理装置が提供され、且つこの情報処理装置において実行されるプログラムについても種々形式の媒体により提供されている。

- 15 特に、ビデオゲーム機器等の情報処理装置においては、実行されるゲームプログラムは、半導体読み取り専用メモリ（ROM）に記憶されてカートリッジに収納された形式、あるいはCD-ROMの形式で提供されることが多い。

- 20 ここで、ビデオゲーム機器業界においては、ビデオゲーム機器本体とともにゲームプログラムの優劣により、その普及が左右される。したがって、優れたゲームプログラムが、正当な権限のない第三者により複写あるいは
25 、模倣され、販売される場合は、ゲームプログラムの開

発者利益を失わせるとともに、顧客の信頼を削ぐ事となる。

そこで、プログラムの真偽性をチェックし、不正なプログラムについては、情報処理装置において、実行を阻止するセキュリティチェック機能を備えることが提案され、且つ実施されている。

たとえば、従来例として米国特許4,442,486（以下486特許と略記する）、4,454,594（以下594特許と略記する）、4,462,076（以下076特許と略記する）あるいは日本国特許出願公開昭公報昭62-3331号（以下331号公報と略記する）等に記載の技術がある。

上記の486特許に記載される技術では、プログラムに特許或いは特許出願等の表示を瞬時間行うための表示信号を生成する内容を含ませ、当該瞬時間表示される内容が装置本体内に記憶している参照信号と一致するか否かにより、プログラムの真偽性を判断するようにしている。

また、594特許に記載される技術も、486特許に記載の技術と同様であり、プログラムを記憶する外部メモリの特定位置に記憶される内容を読み出し、この内容、例えば商標を表示し、次いで本体装置に記憶している参照データと一致するか否かを判断する。そして、これらが一致しない場合は、プログラムの実行が阻止される。

076特許に記載の技術は、上記486特許及び59

4 特許と同様であり、外部メモ리카ートリッジの所定アドレスのデータと本体側の参照データとを比較する。一方、実質的な外部メモリと本体側との接続を行う前に、権利の所有者情報を表示する。

- 5 その後、上記参照データの比較一致がある場合に、外部メモ리카ートリッジを真正なものとしてゲームの実行制御を行うようにしている。

更に、331号公報では、特に本体装置の本来の動作を開始する前に、外部記憶装置において、記憶された真偽判定のためのプログラムを実行させる。同時に本体装置においても真偽判定のためのプログラムを実行させる。これら双方の真偽判定のためのプログラム実行の結果が一致する場合に、本体装置の本来の動作を能動化させるものである。

- 15 このように従来の情報処理装置におけるセキュリティチェックは、ゲームプログラム等のプログラムの実行前にセキュリティコード等の一致を判断することにより行われている。そして、プログラムの実行が開始されると、プログラムの実行中は、セキュリティチェックを行わ
20 ない、若しくは行い得ないものとなる。

このために、プログラムの一連の繋がりにおいて、セキュリティチェック処理のステップが何らかの方法により多くは、不正手段により、不能化されたり、バイパスされた場合には、その後のプログラムのステップの実行
25 がセキュリティチェックなしに可能となるものであった

。

更に、上記 4 8 6 特許、5 9 4 特許或いは 0 7 6 特許におけるセキュリティチェックの方法では、商標等の表示データを瞬時的に表示させているが、単に表示しているのみであり、実際に正しい商標等の画像が表示されているか否かの情報処理装置による判別は、行われていなかったし、行い得る構造ではなかった。

しかも、上記の通りセキュリティチェック処理のステップが何らかの方法により不能化されたり、バイパスされた場合には、所定のデータの表示が行われず、プログラムの真偽の判断が出来なくなるという問題が存在していた。

発明の開示

したがって、本発明の第一の目的は、情報処理装置において実行されるソフトウェア（プログラム）が真正なものか否かを確認することが容易、且つ確実である情報処理装置及びその方法を提供することにある。

更に本発明の第二の目的は、不正なプログラムの製作、販売を法的に確実に防止出来る情報処理装置及びその方法を提供することにある。

また、本発明の第三の目的は、出力データの画像もしくは音声による出力表示が外部記憶装置に記憶されているプログラムに基づくものであるとして、その出力表示が違法性を明示することを可能とする情報処理装置及び

その方法を提供することにある。

- 更にまた、本発明の第四の目的は、プログラムの真正を確認するセキュリティチェック処理をバイパスする不正行為を不能化することを防止し得る情報処理装置及び
- 5 その方法を提供することにある。

また、本発明の第五の目的は、セキュリティチェック処理の途中で不正な（真正でない）プログラムに置き換える不法行為を防止し、上記第四の目的をより確実にする情報処理装置及びその方法を提供することにある。

- 10 更に、本発明の第六の目的は、上記第一乃至第五の目的に適応する外部記憶装置を提供することにある。

- 上記第一の目的に対応する情報処理装置は、プログラム及び出力データが記憶された外部記憶手段と着脱自在に接続されるとともに、外部記憶手段から読み込んだ出力データを表示する出力手段に接続される情報処理装置
- 15 であって、外部記憶手段から読み込んだプログラムを実行するCPUと、基準比較データを記憶する内部記憶手段と、外部記憶手段から読み込んだ出力データと該基準比較データとを比較し、これらが不一致の場合にエラー
- 20 処理信号を発するセキュリティチェック手段とを有することを特徴とするセキュリティチェック機能を有する。

- また、上記第一の目的に対応するセキュリティチェック方法は、プログラム及び出力データが記憶された外部記憶手段からプログラム及び出力データを読み込む第一
- 25 のステップと、外部記憶手段から読み込んだプログラム

に含まれる表示チェック開始命令に基づき、チェック開始信号を出力する第二のステップと、チェック開始信号が出力される時、外部記憶手段から読み込んだ出力データと基準比較データとを比較し、これらが不一致の場合
5 にエラー処理信号を発する第三のステップと、エラー処理信号に基づき、プログラムの少なくとも一部の実行を阻止する第四のステップを有する。

かかる構成において、映像もしくは音声出力として出力表示される出力データがセキュリティチェックの比較
10 対象とされる。これにより真正でないプログラムの実行を確実に阻止することが可能である。

更に、第二の目的に対応する情報処理装置は、前記出力データが、この出力データの前記出力手段への表示が正当な権原を有しない者の使用を禁止し得るものである
15 ことを特徴とする。

また、上記第二の目的に対応するセキュリティチェック方法は、前記第三のステップにより、前記出力データと基準比較データとが一致する時に、前記出力データを表示する制御信号を発生し、更に、この制御信号に基づ
20 き出力データを表示する第五のステップを有することを特徴とする。

かかる構成により、出力データが商標等である場合、その表示が正当な権原を有しない者の使用を禁止し得るものであり、したがって不正なプログラムの製作、販売
25 を法的に禁止することが可能である。

更にまた、上記第三の目的に対応する情報処理装置は、前記基準比較データと比較される出力データを格納する出力データ格納手段を有し、出力データは前記外部記憶手段に記憶されたプログラムに従って、外部記憶手段から出力データ格納手段に転送され格納される。

また、上記第二の目的に対応するセキュリティチェック方法は、前記第一のステップにより、前記外部記憶手段に記憶される出力データを、前記プログラムに従って、読み込むことを特徴とする。

10 かかる構成により、外部記憶装置に記憶されているプログラムに従って、出力データがデータ格納手段に転送され、格納されるので、出力データの出力表示が外部記憶装置に記憶されているプログラムによるものであり、違法性を明確化させることが可能である。

15 更に、上記第四の目的に対応する情報処理装置は、前記セキュリティチェック手段が、前記CPUの動作中に、前記出力データと基準比較データとの比較を繰り返して行うことを特徴する。

また、上記第四の目的に対応するセキュリティチェック方法は、前記第三のステップにより、前記出力データと基準比較データとの比較が前記プログラムの実行中に繰り返されることを特徴とする。

かかる構成により、プログラムの実行中にセキュリティチェックのための比較が繰り返し実行されるので、セキュリティチェックをバイパスする等の不正行為を防止

できる。

また、上記第五の目的に対応し、情報処理装置は、前記出力データが、前記セキュリティチェック手段によるデータ比較が行われる前に前記外部記憶手段から前記出力データ格納手段に転送され記憶され、セキュリティチェック手段によるデータ比較及び前記出力手段による出力表示の後、該出力データ格納手段から消去される。

上記第五の目的に対応するセキュリティチェック方法は、前記第五のステップによる出力データの表示の後に、読み込んだ該出力データを消去する第六のステップを有する。

かかる構成により、繰り返しの比較チェックのために新たに出力データを読み込むことが必要となる。したがって、セキュリティチェック処理の途中で不正な（真正でない）プログラムに置き換える不法行為が防止され、上記第四の目的をより確実に達成する。

更に、本発明の第六の目的に対応する情報処理装置に着脱自在に接続される外部記憶装置では、情報処理装置において実行されるプログラムと、情報処理装置により表示制御される出力データを有し、出力データはこのプログラムに従って、情報処理装置への読み込みが制御される。

かかる構成により、外部記憶装置は、上記第一乃至第五の目的に適応可能となる。

図面の簡単な説明

図 1 は、本発明の実施例ブロックである。

図 2 は、表示制御部の構成例を示すブロックである。

図 3 は、CPU の動作フローである。

5 図 4 は、表示チェック部の動作フロー（その 1）である。

図 5 は、表示チェック部の動作フロー（その 2）である。

図 6 は、表示制御部の制御部の動作フローである。

10 図 7 は、表示データ格納部の構成例ブロックである。

図 8 A、図 8 B は、表示データの説明のための図であり、図 8 A は表示パターンの一例を示し、図 8 B は、当該表示パターンに対応するメモリの b i t 情報を示す。

図 9 は、カラー表示データの表示方法を説明する図で
15 ある。

図 1 0 は、本発明の他の実施例であるビデオ信号制御回路の構成を示す図である。

図 1 1 は、図 1 0 のビデオ信号制御回路により表示制御されるセキュリティチェックのための表示ロゴの一例
20 を示す図である。

発明を実施するための最良の形態

以下、好ましい実施例を図面に従い説明する。尚、図において、同一または類似の部分には、同一の参照番号
25 または記号を付して説明する。

図 1 は、本発明の一実施例の構成ブロック図であり、
実施例として情報処理装置をゲーム機に適用した場合に
ついて示す。図において、1 は、情報処理装置本体とし
てのゲーム機本体であり、バス B S を通して C P U 1 0
5 、比較用基準データ格納メモリ 1 1、表示チェック部 1
2、表示データ格納部 1 3、表示制御部 1 4、ビデオデ
ィスプレイプロセッサ (V D P) 1 5 及び作業用メモリ
1 6 が接続されている。

2 は、外部記憶装置としてのゲームカートリッジであ
10 り、コネクタによりゲーム機本体 1 と着脱可能に接続さ
れる。ゲームカートリッジ 2 は、内部に R O M を収納し
、ゲーム実行のためのデータ格納領域 2 1 とゲームプロ
グラム格納領域 2 0 を有している。

尚、以下の説明において、ゲームカートリッジ 2 及び
15 内部に収容される R O M として説明するが、これは C D
駆動装置及び C D - R O M に置き換えることも可能であ
る。

データ格納領域 2 1 は、主にゲーム実行時に表示され
るキャラクタ等のデータを格納するデータ部 2 1 1 と、
20 本発明にしたがいセキュリティチェックのために表示さ
れる表示データを格納する表示データ部 2 1 2 を有する
。

ここで、表示データは、後に説明するようにゲーム機
本体 1 で使用される真正なプログラムであることを意味
25 するデータであり、例えばゲーム機本体 1 の製造者の商

- 1 1 -

標等の画像に関するデータ、あるいは、音声による表示データである。

また、必要に応じてより高いセキュリティ性を持たせるために表示データを圧縮して格納することも可能である。

更に、ゲームプログラム格納領域 20 に記憶されるゲームプログラムには、その一部として、本発明にしたがい、CPU 10 の制御の下に、少なくとも表示データ部 212 から表示データを読み出し、ゲーム機本体 1 の表示データ格納部 13 に転送し記憶させる制御命令が含まれている。

上記のように表示データを圧縮して表示データ部 212 に格納する場合は、この圧縮表示データを解凍するための解凍プログラムがゲームプログラム格納領域 20 にゲームプログラムの一部として格納されてもよい。また、ハードウェアにより解凍を行う場合は、ゲーム機本体 1 もしくは、ゲームカートリッジ 2 に解凍回路を設ける構成とすることが可能である。

図 1 において、更に 3 は表示装置である。表示装置 3 は、ゲーム機本体 1 の表示制御部 14 からの映像信号を受け、表示部に所定の表示を行う。特に、本発明にしたがいゲームカートリッジ 2 から読み出し、転送記憶した表示データ 30 が表示装置 3 の所定位置に表示される。

尚、以下実施例において、本発明のセキュリティチェックのための表示データの表示を画像として表示装置 3

に表示する場合を例に説明するが、本発明はこれに限定されない。

即ち、先に説明したように、ゲーム機本体 1 で使用される真正なプログラムであることを意味するデータとして映像データの他、音声データも含まれる。したがって、音声データである場合は、音声出力によりデータが表示されることは、言うまでもない。

表示制御部 1 4 の詳細と、表示装置 3 を含む本発明にしたがう表示データ 3 0 を表示するための構成が、更に図 2 に示される。図 2 において、表示制御部 1 4 は、制御部 1 4 0、セレクト 1 4 1 及び D/A 変換回路 1 4 2 を有して構成される。

図 3 乃至図 6 は、それぞれ CPU 1 0、表示チェック部 1 2 及び表示制御部 1 4 の制御部 1 4 0 の動作フローである。以下これらの動作フローを参照しながら、図 1、図 2 の詳細について更に説明する。

図 3 において、ゲームの開始に際し、ゲーム機本体 1 の図示しない電源スイッチが投入されると（ステップ S 1）、CPU 1 0 は、ゲームカートリッジ 2 のプログラム格納領域 2 0 からゲームプログラムを読み込み、ゲーム処理を行う（ステップ S 2）。

CPU 1 0 に読み込まれたゲームプログラムには、所定タイミングで表示チェック開始を指示する命令が含まれている。したがって、CPU 1 0 はこの表示チェック開始命令の有無をチェックする（ステップ S 3）。

ここで、表示チェック開始のタイミングは、システムとして任意に設定可能である。例えば、ゲーム進行の過程でのゲームシーンの切り替わり時を表示チェック開始のタイミングとしてゲームプログラムに命令を記述しておくことが可能である。

表示チェック開始の命令があると（ステップ S 3 : Yes）、CPU 10 は、読み込まれたゲームプログラムに記述される格納命令を実行する（ステップ S 4）。即ち、ゲームプログラムの格納命令にしたがい、ゲームカートリッジ 2 の表示データ格納領域 21 から表示データを読出し、表示データ格納メモリ 13 に転送し、記憶する。

次いで、CPU 10 は、表示チェック部 12 にチェック許可信号を出力する（ステップ S 5）。このチェック許可信号には、チェック開始信号、データ種類、データサイズ、表示位置情報が含まれている。

CPU 10 からのかかる動作が、ゲームが終了するまで繰り返される（ステップ S 6）。

ここで、データ種類は、比較用基準データメモリ 11 に予め複数種の基準データが記憶されており、その内の一種の種類の基準データを特定する情報である。データサイズは、表示データ 30 を表示装置 3 に表示する際に、そのサイズを可変に出来る機能を有している場合に、そのサイズを指定する情報である。

更に、表示位置は、表示データ 30 を表示装置 3 に表

示する際に、その表示位置を可変にできる機能を有する時、その表示位置を指定する情報である。

図 4 は、チェック開始信号、データの種類、データサイズ、表示位置情報が含まれるチェック許可信号を CPU 10 から受ける表示チェック部 12 の第一の動作フローである。

表示チェック部 12 は、基本構成として、タイマーカウンタ機能と比較回路機能を有する専用のロジック回路あるいは、CPU により構成される。ゲーム機本体 1 の電源が投入されると動作を開始し、タイマーカウンタの計数をスタートする（ステップ S 20）。

表示チェック部 12 をロジック回路で構成する場合は、CPU 10 からのチェック許可信号の入力をトリガとしてセキュリティチェック（データ比較）のための比較論理が求められる。また CPU で構成する場合は、データ比較プログラムをゲーム機本体 1 の ROM（図 1 においては、図示省略されている）に格納しておき、CPU 10 からのチェック許可信号の入力をトリガとして、表示チェック部 12 において、このデータ比較プログラムを実行してセキュリティチェック（データ比較）が行われる。

ついで、タイマーカウンタがウォッチドグタイマーの機能を果たし、所定計数値、即ち所定時間が経過したか否かが判断される（ステップ S 21）。

タイマーカウンタが所定計数値まで既に到達している

場合には、所定期間においてCPU 10が、ゲームカートリッジ2のプログラム格納領域20から正しくプログラムを読み出せないことを示す。あるいは、プログラムが真正のものではなくプログラムにセキュリティ解除ルーチンを有してなく、またはセキュリティを解除するキーデータ（表示データ）を有していないためにセキュリティを正当に解除できない状態にあることを示す。

この場合は、エラー処理の対象となる（ステップS28）。エラー処理の対象となる場合は、それ以降セキュリティチェックは行われず、表示チェック部12はエラー処理信号として例えば、CPU 10に対してホルト信号を発する。これによりCPU 10は動作を停止し、ゲームプログラムの実行が不能となる。

一方、ステップS21の判断において、タイマーカウンタが所定計数値に到達していない場合は、CPU 10から許可信号が送られているか否かが判断される（ステップS22）。CPU 10から許可信号が送られていない場合は、継続してタイマーカウンタが計数アップされる（ステップS23）。

20 一方、許可信号が送られている場合は、セキュリティチェックが開始される（ステップS24）。ここで、セキュリティチェックは、本発明にしたがい次のように行われる。

図1において、ゲームカートリッジ2に収容されるROM内のプログラム格納領域20に記憶されるゲームプ

プログラムに含まれる命令により、CPU 10は、表示データ部 212の表示データを読み出し、RAMで構成される表示データ格納部 13に転送記憶する。

同時に、CPU 10は、ゲームプログラムに含まれる
5 チェック開始命令に基づき、データ種類、データサイズ、表示位置情報を含むチェック開始信号を表示チェック部 12に送る。

データ種類、データサイズ、表示位置情報の意義は、既に説明した通りである。更に、表示データは、たとえ
10 ば、同じ意味のセキュリティの表示であっても、ゲーム機器が使用される国の言葉に対応して表示することが必要である場合がある。

このために、データ種類は、当該ゲームカートリッジ 2の表示データ部 212に記憶される表示データが、異なる国の言葉に対応する複数種の表示データのいずれであるかを指定する情報をも含む。したがって、ゲーム機
15 本体 1のROMで構成される比較基準データ格納部 11には、複数種の比較基準データが記憶されている。

ここで、表示チェック部 12から表示制御部 14に出力される表示データの内、特にデータサイズ及び表示位置データは、これを不正に操作することにより、目視できないサイズや画面に表示しきれないサイズにしたり、表示装置 3の有効画面外に表示位置を移動することが可能である。

25 このためにリミッタを設け、かかるデータサイズ及び

表示位置に対する不正操作を防止することが望ましい。
このリミッタの設定により、表示装置 3 の画面に収まり
切れない過大なデータサイズや目視可能な最小のデータ
サイズに満たないデータサイズが表示チェック部 1 2 か
5 ら出力された場合に、これを表示装置 3 の画面内に収ま
り目視可能な適当なデータサイズに置き換える機能を有
する。

図 4 の動作フローに戻ると、表示チェック部 1 2 にお
いて、CPU 1 0 から送られるデータ種類が特定する比
10 較基準データを比較基準データ格納部 1 1 から読出し、
表示データ格納部 1 3 に転送記憶された表示データとの
比較チェックが開始される（ステップ S 2 4）。

比較チェックの結果、比較基準データと表示データ格
納部 1 3 に転送記憶された表示データが一致しない場合
15 は、ゲームカートリッジ 2 は、真正なものとは判断され
ず、エラー処理（ステップ S 2 8）の対象となる。

このエラー処理は、先に説明したタイマーカウンタが
所定計数値に到達している場合（ステップ S 2 1 : Y e
s）の処理と同様であり、強制的に CPU 1 0 の動作を
20 停止する。これにより、以降のゲームプログラムの実行
が阻止される。

一方、比較チェックの結果、比較基準データと表示デ
ータが一致する場合は、ゲームカートリッジ 2 は、真正
なものと判断される。次いで、表示データ格納部 1 3 に
25 転送記憶されている、ゲームカートリッジ 2 の表示デー

タ領域 2 1 2 からの表示データが所定時間経過後に消去される（ステップ S 2 6）。

このように表示データが消去されるのは、次の理由にある。表示データを消去しない場合は、最初に表示データが表示データ格納部 1 3 に格納されると、それ以降何度セキュリティチェック（データの比較）を繰り返しても常にチェック結果は、「データの一致」ということになる。

したがって、本発明に従い、プログラムの実行中に繰り返しセキュリティチェックをする意義がなくなる。その結果、途中で何らかの不正行為により、不正な（真正でない）プログラムが実行される虞がある。これにより、上記の通り表示データの消去により、かかる不正行為を禁じることが可能である。

15 尚、この表示データの消去は、データ比較で一致が確認されてからモニタ画面で遊戯者がその表示を容易に確認できる程度の所定時間経過後に行われる。また、表示データの消去は、プログラムの改ざん等による抜け道をより確実に防止するために、専用の回路を本体装置 1 側に設け、ハード的に強制に行われることが好ましい。

ここで、上記の表示データの消去は、表示データ格納部 1 3 に格納された表示データをクリアーすること即ち、オール“0”のパターンを書き込みことにより、あるいは、先に格納されている表示データと異なるパターン
25 のデータを書き込むことにより可能である。

更に、上記の表示データの消去の際、タイマーカウンタがリセットされ（ステップS 2 7）、フローの始まり（ステップS 2 0）に戻り、タイマーカウンタの初期値からのカウントを再開始する。

- 5 従って、タイマーがタイムアップする前にセキュリティチェックが繰り返し実行され、表示データと比較基準データとが一致している間は、エラー処理（ステップS 2 8）が行われることはない。逆に、タイムアップ前にチェック許可信号がなければ、不正プログラムと判断され、エラー処理が行われる。

以上説明した実施例においては、チェック許可信号がCPU 1 0から表示チェック部1 2に送られる都度、所定時間内に繰り返し、セキュリティチェックが行われる。

- 15 尚、図4の動作フローでは、ステップS 2 1において、タイマーカウンタが所定値に到達している場合には、ただちにエラー処理（ステップS 2 8）を行うようにしている。これに対して、図5に示す別の実施例動作フローのように、タイマーカウンタが所定値に到達している場合であってもチェックを開始し（ステップS 2 4）、表示データの一致判断（ステップS 2 5）を行うようにしてもよい。

- 25 真正でないゲームプログラムにより、タイマーカウンタが所定値に到達している場合は、セキュリティチェックの結果においても、表示データの一致とはならずエ

- 2 0 -

ラー処理（ステップS 2 8）を行うことになる。他の動作については、図 4 の動作フローの実施例と同様である。

ここで、上記の通り、表示チェック部 1 2 における比較基準データと表示データとの比較チェックの結果が、両者が一致するものである場合、ゲームカートリッジ 2 に格納されるゲームプログラムは、真正なものに見做される。

一方、ゲームプログラム自体が不法にコピーされたものである場合も、上記の表示チェック部 1 2 における比較結果は、両者が一致するものとなる。したがって、かかる場合も後に続くゲームプログラムの実行が可能となる。

しかし、この場合は、表示データを表示装置 3 に表示させること自体が、正当な権原を有しない者に対し、禁止しうるもの、例えば、商標等の表示データとすることにより、不法なコピー行為を禁止することが可能となる。

何故ならば、正当な権原を有しない者による商標等の表示データを表示装置 3 に表示させる行為は、明らかな商標等に基づく権利侵害となるからである。

図 6 は、表示制御部 1 4 内の制御部 1 4 0（図 2 参照）の動作フローである。先に図 1 に関して説明したように、CPU 1 0 から表示チェック部 1 2 に対し、チェック開始信号が送られる際に、データ種類、データサイズ

、表示位置情報が送られる。

表示チェック部 1 2 は、チェック開始信号に基づき表示オン／オフ信号とともにデータサイズ、表示位置情報 1 2 0 を表示制御部 1 4 内の制御部 1 4 0 に送る。表示
5 制御部 1 4 は、表示データ格納部 1 3 からの表示データを映像信号 1 3 0 として入力する。

更に、表示制御部 1 4 は、ビデオディスプレイプロセッサ (VDP) 1 5 からゲーム画像データを映像信号 1 5 0 として入力する。表示制御部 1 4 において、表示データ格納部 1 3 からの映像信号 1 3 0 と VDP 1 5 からの映像信号 1 5 0 は、セクタ 1 4 1 に入力される。
10

ここで、本発明と直接に関連しないので、ビデオディスプレイプロセッサ (VDP) 1 5 の詳細な構成及び動作の説明は、省略するが、既存のビデオゲーム装置において使用される周知構成のデバイスであり、CPU 1 0
15 に対し、I/O デバイスとして存在する。レジスタ、カラー RAM、スクロール量設定 RAM 等を有し、これらとともに更に外部に付属されるビデオ RAM を制御する制御ブロックを有して構成され、表示装置 3 に表示され
20 るビデオ画像データを合成して映像デジタル信号として出力する。

また VDP 1 5 からは、垂直、水平同期信号 1 5 2 が映像デジタル信号と同期して出力され、制御部 1 4 0 に入力される。制御部 1 4 0 は、表示チェック部 1 2 からの表示オン／オフ信号に基づき、同期信号 1 5 2 に同期
25

- 2 2 -

してセレクト信号 1 4 3 を出力する。

このセレクト信号 1 4 3 は、セクタ 1 4 1 に入力され、映像信号 1 3 0 と 1 5 0 を切替え出力するためのものである。この切替え動作は、図 6 の動作フローに対応して説明される。

5 10 15 20 25
まず、制御部 1 4 0 は、表示チェック部 1 2 からの表示オン／オフ信号がオンか否かを判断する。表示オン／オフ信号がオンである場合は、表示データ格納部 1 3 からの表示データの映像信号を表示するタイミングであるか否かが判断される（ステップ S 3 1）。

このステップ S 3 1 における判断は、表示チェック部 1 2 からの表示データのデータサイズ、表示位置信号 1 2 0 に基づき且つ、VDP 1 5 からの同期信号 1 5 2 をもとに表示データの表示タイミングか否かが判断される。

表示データの表示タイミングである場合は、セレクト信号 1 4 3 により表示データ格納部 1 3 からの表示データの映像信号 1 3 0 が選択される（ステップ S 3 2）。一方、表示データの表示タイミングでない場合は、セレクト信号 1 4 3 により VDP 1 5 からの映像信号 1 5 0 が選択される（ステップ S 3 3）。

このようにして、セレクト信号 1 4 3 により選択され、セクタ 1 4 1 から表示データの映像信号 1 3 0 及び VDP 1 5 からの映像信号 1 5 0 が出力され、次いで D / A 変換回路 1 4 2 に入力する。

D/A変換回路142は、デジタル信号である映像信号130及び映像信号150をアナログ映像信号144に変換する。そしてこの変換されたアナログ映像信号144は、同期信号152とともに表示装置3に入力され、所定の表示が行われる。

尚、上記ステップS32において、表示チェック部12からの表示データの表示タイミングと、表示チェック部12におけるセキュリティチェック（データの比較）とは、必ずしも一対のものである必要はない。表示チェック部12におけるセキュリティチェックは、比較的短時間の間隔で行い、画面の表示は、その表示をしても支障の無い時に、表示チェック部12におけるセキュリティチェック後に表示するようにしてもよい。

この制御のためには、例えば、表示チェック部12において、表示制御部14に送る表示オン/オフ信号120の送出タイミング、あるいは表示制御部14の制御部140からのセレクト信号143の出力タイミングを予め所定の制御周期に設定することにより可能である。

図7乃至図9は、表示データの一例に基づき、表示データ格納部13の構成及び表示データの表示方法を説明する図である。

図7に示すように表示データ格納部13は、RAMで構成されるメモリ131とシフトレジスタ133で構成される。メモリ131は、表示チェック部12からのアドレス信号120が順次入力される。シフトレジスタ1

- 2 4 -

3 3 には、表示チェック部 1 2 からのラッチ信号及びシフト信号 1 2 1 が入力される。

ここで、今、図 8 A に示すように、表示データのパターンが "S" である場合を考える。図 8 A の 7 ~ 0 ビットとアドレス 0 ~ 7 によって特定される 6 4 画素で構成される 8 × 8 のマトリクスの範囲が表示データ領域である。

この 8 × 8 のマトリクスの範囲中、黒点により表示データのパターン "S" が表されている。この表示パターンに対応して、メモリ 1 3 1 のビット情報が図 8 B のように表される。即ち、表示データのパターン "S" を形成する黒点に対応して、メモリ 1 3 1 の対応するビット位置は、"1" にセットされている。

図 7 に戻り、表示チェック部 1 2 からアドレス 1 2 0 として、アドレス信号 (3) がメモリ 1 3 1 に入力する場合を考えると、メモリ 1 3 1 の対応するアドレスのビット情報即ち、"0 0 1 0 0 0 0 0" がデータ 1 3 2 として読み出される。

これが表示チェック部 1 2 からのラッチ信号によってシフトレジスタ 1 3 3 にラッチされ、ラッチされたデータ 1 3 2 は表示チェック部 1 2 からのシフト信号によって 7 ビット目を先頭に順次 1 ビットずつ表示制御部 1 4 に映像信号 1 3 0 として送られる (図 7、1 2 1 参照)。

この映像信号 1 3 0 は、表示制御部 1 4 において、す

でに説明したようにセクタ 1 4 1 を通して表示装置 3 に表示データ 3 0 として表示される。

図 9 は、表示データをカラー表示する場合の表示データ格納部 1 3 のメモリ 1 3 1 とシフトレジスタ 1 3 3 の構成を説明する図である。表示データを構成する各ビットに対し、R : G : B の組み合わせで所定の色が表示される。

したがって、図 8 B のビット情報を R : G : B 用に 3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B として用意する。更に、シフトレジスタ 1 3 3 は、3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B のそれぞれに対応してシフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B が用意される。

所定の色を構成する R : G : B ごとに 3 枚のメモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B の所定アドレスとビットに対応するビット位置に "1" がセットされる。したがって、メモリ 1 3 1 - R、1 3 1 - G、1 3 1 - B のそれぞれからビット情報が読み出されてシフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B にラッチされる。

シフトレジスタ 1 3 3 - R、1 3 3 - G、1 3 3 - B にラッチされた R : G : B ごとのビット情報は、図 7 で説明したと同様にカラー映像情報として表示制御部 1 4 に送られる。

表示制御部 1 4 においては、図 2 において説明したと

同様にして表示装置 3 にカラー映像情報が送られ、これにより表示装置 3 において、表示データがカラー表示される。

尚、上記実施例において、エラー処理時に表示チェック部 12 が発するエラー処理信号としては、上述したホル
5 ト信号の他に CPU 1,0 に対するリセット信号やゲーム装置本体 1 全体を対象とするシステムリセット信号とすることも可能である。

但し、これらのリセット信号をエラー処理信号として
10 表示チェック部 12 が出力する場合には、リセット後に不正プログラムが再実行されることを防止するために、そのエラー処理信号出力が継続的に保持されることが望ましい。

上記したように、先の実施例では、商標等の表示データと比較基準データとの比較の結果一致する場合に、表示
15 を行うことを前提としている。これに対し、図 10 は、他の実施例として、基準比較データとカートリッジ 2 から読みだした表示データとの比較チェックが開始されると所定時間、読みだした表示データが真正なデータであるか否かに関わらず表示装置 3 への表示を継続する
20 ように制御するビデオ信号制御装置の構成例を示す。かかる構成により、より明確に観察者に表示データが表示されていることの認識が容易となる。

図 10 に示すビデオ信号制御装置は、具体例として半
25 導体の 1 チップ上に形成され、太い破線 5 に囲まれたビ

ビデオ信号制御回路 5、アドレスデコーダ 6、VDP 15
(図 1 参照)からの表示データが入力される FIFO メ
モリ 7、ピクセルフォーマット変換回路 8 及びデジタル
アナログ変換回路 9 を有して構成される。

- 5 更に、ビデオ信号制御回路 5 は、データ表示用回路 5
0、セキュリティチェック開始制御回路 51、データ比
較回路 52 及びセキュリティロックタイマー 53 を有す
る。

図 10 においては、ゲーム機本体を構成するためにビ
10 デオ信号制御装置に接続される、図 1 に示される CPU
10、ワークメモリ 16 及び VDP 15 に相当する回路
装置は、図示省略されている。

図 10 の動作は、基本的に先の図 1 の実施例と同様で
あるが、固有の動作特徴を有する。したがって、必要に
15 より図 1 を参照しながら図 10 の動作を以下に説明する
。

デジタルアナログ変換回路 9 は、図 2 において説明し
た表示制御部 14 (図 1 参照)のデジタルアナログ変換
回路 142 に対応し、基本的機能としてデジタルのビデオ
20 オ信号をアナログビデオ信号に変換して表示装置 3 に R
GB 信号を送る回路である。

更に、図 10 のデジタルアナログ変換回路 9 は、VDP
15 からのビデオ信号を FIFO メモリ 7 及びピクセル
フォーマット変換回路 8 を通して入力するとともに、
25 後に説明するデータ表示用回路 50 の出力を入力する。

これらを表示装置 3 に表示するためのアナログビデオ信号に変換する機能を有する。

図 1 0 において、セキュリティカーソル格納用 R O M 1 1 0 は、図 1 の比較用基準データを記憶する書き込み
5 専用メモリ 1 1 に相当する。ここでセキュリティカーソルとして表示されるロゴは、一例として図 1 1 に示すごとく 3 2 × 1 6 画素の単色で表される S E G A の表示である。

カラーレジスタ 1 1 1 及び、1 1 2 は、このセキュリティ
10 カーソルを構成する画素の内、それぞれ“1”の画素及び“0”の画素のカラーを指定する情報を格納するレジスタである。

例えば、“1”の画素は、黒字に青で表示され、“0”の画素は黒地と同色に表示される。これらの色を特定
15 するコードが、セキュリティカーソルを構成する画素数分がカラーレジスタ 1 1 1 及び、1 1 2 に格納される。カラーレジスタ 1 1 1 及び、1 1 2 は、セキュリティカーソル格納用 R O M 1 1 0 と同様に読出専用のメモリで構成され、セキュリティカーソル格納用 R O M 1 1 0 及
20 びカラーレジスタ 1 1 1、1 1 2 には、上記セキュリティカーソル及び対応する画素のカラー指定情報が 予め格納されている。

参照数字 6 は、C P U 1 0 から送られるアドレス信号をデコードしてビデオ信号制御装置における対象となる
25 回路に対し、イネーブル信号を送り動作を活性させるデ

コード回路である。

ここで、ゲームカートリッジ 2 に収容される R O M 内のプログラム格納領域 2 0 に記憶されるゲームプログラムに含まれる表示チェック命令を C P U 1 0 が検知すると、C P U 1 0 からデータ表示用回路 5 0 の後に説明する各メモリを指定する C P U アドレスとともに、ゲームカートリッジ 2 から読み込んだ表示データが C P U データとしてビデオ信号制御装置に送られる。

図 1 0 のビデオ信号制御装置において、データ表示用回路 5 0 が図 1 の表示データ格納部 1 3 に対応する。データ表示用回路 5 0 は、C P U 1 0 から送られる表示データ中のセキュリティカーソルのビットマップパターンを記憶するカーソル R A M 1 3 0 を有する。更に C P U 1 0 から送られる表示データ中には、セキュリティカーソルの表示位置及び表示カラー指定情報が含まれている。したがって、データ表示用回路 5 0 には、更にこれらの情報を格納する X、Y ポジションレジスタ 1 3 1、1 3 2 及びカラーレジスタ 1 3 3、1 3 4 を有している。

ここでアドレスデコーダ 6 は、C P U 1 0 から送られる表示データ格納部 1 3 即ち、データ表示用回路 5 0 を指定する C P U アドレスを受信する。アドレスデコーダ 6 は、これをデコードし、カーソル R A M 1 3、X、Y ポジションレジスタ 1 3 1、1 3 2 及びカラーレジスタ 1 3 3、1 3 4 を活性化するトリガ信号であるイネーブル信号を出力する。

- 3 0 -

イネーブル信号は、5つのオアゲート102を通して、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134に送られる。

- 5 したがって、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134は、それぞれ、CPUデータである表示データ中のセキュリティカーソルの表示パターン、その表示位置及び表示カラー情報を格納することが可能となる。
- 10 したがって、カーソルRAM130、X、Yポジションレジスタ131、132及びカラーレジスタ133、134に格納された表示データは、デジタルアナログ変換回路9に導かれる。

- ここで、カーソルRAM130に格納されたビットマップデータで構成されるセキュリティカーソルのロゴが、各画素がカラーレジスタ133、134に格納されたカラー指定コードに対応するカラーを有し、X、Yポジションレジスタ131、132に格納されたデータで指定される表示位置に、表示が行われるようにアナログビデオ信号に変換されて表示が開始される。
- 15
- 20

- ここで、カーソルRAM130に格納されたセキュリティカーソルを構成するビットマップの各ビットの上記カラーレジスタ133、134に格納されたカラー指定コードに対応するカラー表示は、次のように行われる。
- 25 セキュリティカーソルを構成するビットの論理値が“0

”である時、カラーレジスタ 1 3 3 の出力が選択され、
反対にビットの論理値が “ 1 ” である時、カラーレジスタ 1 3 4 の出力が選択され、それぞれのカラーレジスタにより指定されるカラーコードに対応する R G B 信号に
5 変換される。

更に、カーソル R A M 1 3 0、X、Y ポジションレジスタ 1 3 1、1 3 2 及びカラーレジスタ 1 3 3、1 3 4 への表示データ等の格納が完了し、上記のようにセキュリティカーソルの表示が開始されると、C P U 1 0 は、
10 チェックスタート駆動回路 1 0 0 を選択する C P U アドレス信号をアドレスデコーダ 6 に送る。したがってチェックスタート駆動回路 1 0 0 が選択されチェックスタート信号を出力する。

次いで、チェックスタート信号を契機としてセキュリティ
15 ティチェックタイマー 1 0 1 が、計数を開始する。セキュリティチェックタイマー 1 0 1 の出力は、所定の計数値まで計数する間は、オア回路 1 0 2 を通して C P U 1 0 からの各回路への新たな書き込みを禁止する論理値を出力する。

20 したがって、タイムアップまでの所定時間上記のようにデータ表示用回路 5 0 からの同じ表示データの出力により同じセキュリティカーソルの表示が継続する。セキュリティチェックタイマー 1 0 1 が計数完了（タイムアップ）した時、C P U データの新たな書き込みの禁止が
25 解除される。

即ち、セキュリティチェックタイマー 101 は、セキュリティチェック開始と同時に動作し、チェック開始からタイムアップまでの所定時間（実施例として約 1 秒）カーソル RAM 130 に対する書き込みを禁止する。

5 この結果、カーソル RAM 130 に格納されている表示データが上記所定時間継続して表示される。これにより、比較チェック終了までの間だけ真正な表示データをカーソル RAM 130 に書き込み、画面表示が視認され前に、データを書き換えることが出来なくなる。

10 したがって、不正ソフトであっても、チェック開始後、商標等のロゴが所定時間表示されることになる。この不正ソフトによるロゴの表示は、明らかに商標侵害、あるいは不正競争行為を構成するものである。

一方、チェックスタート駆動回路 100 からのスタート
15 ト信号は、同時にデータ比較回路 52 の各要素回路に対してトリガ信号として与えられる。したがって、比較回路 12 は、このトリガ信号を契機としてデータ表示用回路 50 のカーソル RAM 130 及びカラーレジスタ 133、134 に格納された表示データと、データ比較回路
20 52 のセキュリティカーソル RAM 110 及びセキュリティカラーレジスタ 111、112 からの比較基準用セキュリティデータを読み込み、これらを比較する。比較回路 12 は、一致を検知する場合、論理“1”、不一致の時は論理“0”を出力する。

25 更に、データ比較回路 52 において、X ポジションチ

- 3 3 -

5 ェック回路 1 3 5 及び Y ポジションチェック回路 1 3 6
を有し、それぞれデータ表示用回路 5 0 の X ポジション
レジスタ 1 3 1、Y ポジションレジスタ 1 3 2 からセキ
ュリティカーソルの表示開始位置の X 座標位置及び Y 座
5 標位置のデータを読み込み、予め設定されている許容表
示範囲即ち、X ポジション範囲及び Y ポジション範囲と
比較する。

10 X 座標位置及び Y 座標位置のデータが許容表示範囲に
ある時は、X ポジションチェック回路 1 3 5 及び Y ポジ
ションチェック回路 1 3 6 からそれぞれ論理 “1” が出
力される。許容表示範囲にない時は、論理 “1” が出力
される。

15 アンド回路 1 3 7 は、比較回路 1 2、X ポジションチ
ェック回路 1 3 5 及び Y ポジションチェック回路 1 3 6
からの出力が入力され、これら全ての論理が “1” であ
る時、カートリッジ 2 は真正なプログラム 2 0 を格納し
ていると判断出来る。

20 この時、アンド回路 1 3 7 はタイマー初期化信号を出
力し、セキュリティロックタイマー 5 3 の計数値を初期
値例えば “零” に戻し、再び計数を開始する。これによ
りセキュリティロックタイマー 5 3 の計数が所定の計数
値に達するまでの時間が延長される。

25 このようにセキュリティロックタイマー 5 3 は、セキ
ュリティカーソルを視認可能に所定時間表示するために
設けられているセキュリティチェックタイマー 1 0 1 と

異なり、プログラムの実行中に繰り返しセキュリティチェックの実行を行わすために設けられてる。そして、真正ソフトが使用されている間は、タイムアップ前に必ずリセットされる（初期値に戻される）ので、常に作動状態（計数状態）とされる。

この為に、真正ソフトは、セキュリティロックタイマー 53 がタイムアップする前に、セキュリティチェックが行われるように作成されている。尚、実施例として、途中にリセットされない時にセキュリティロックタイマー 53 がタイムアップするまでの所定時間は、約 15 分に設定される。

比較チェックの結果が不一致であった場合は、リセットされないでタイムアップし、デジタルアナログ変換回路 9 に対して表示オフ信号を出力する。これにより下記に説明するように、全ての表示が不能となる。

また、真正な表示データをカーソル RAM 130 に書き込まないようにする等の不正処理を行う不正ソフトの場合にも、セキュリティロックタイマー 53 は、リセットされない。このため、同様にセキュリティチェックタイマー 101 のタイムアップ前に、セキュリティロックタイマー 53 がタイムアップして表示オフ信号が出力が出力されて、全ての表示が禁止される。

データ表示用回路 50 のカーソル RAM 130 の出力は、VDP 15（図 1 参照）から出力される表示データより最優先のビットマップデータとして予め設定されて

いる。したがって、セキュリティロックタイマー 5 3 が所定の計数値に達するまでの期間、カーソル R A M 1 3 0 に格納されるセキュリティ表示のロゴデータ、例えば図 1 1 に示すようなロゴマークが、X、Y ポジションレジスタ 1 3 1、1 3 2 で特定される位置にカラーレジスタ 1 3 3、1 3 4 で特定されるカラーで表示される。

一方、アンド回路 1 3 7 の入力のいずれかが論理 " 0 " である場合は、カートリッジ 2 に格納されるプログラム 2 0 は不正なものであると判断する。

10 かかる場合は、アンド回路 1 3 7 から初期化信号は出力されずに、セキュリティロックタイマー 5 3 は、計数をそのまま継続する。そして、所定の計数値まで達した時、デジタルアナログ変換回路 9 から表示オフ信号が出力される。

15 表示オフ信号は、デジタルアナログ変換回路 9 に入力され、F I F O メモリ 7 及びピクセルフォーマット 8 を通してデジタルアナログ変換回路 9 に入力される、V D P 1 5 から出力されたビデオ信号のアナログビデオ信号への変換を阻止する。

20 これにより、セキュリティチェックによりカートリッジ 2 に格納されるプログラム 2 0 が不正なものであると判断される場合は、V D P 1 5 から出力されるビデオデータ信号は表示が禁止され、以降のゲームの継続が不可能となる。

25 尚、上記図 1 0 の実施例において、デジタルアナログ

変換回路 9 の回路の一部としてデータ比較回路 5 2 の機能を一体にして構成することが可能である。この場合は、アナログビデオ信号に変換される直前即ち、表示装置 3 に対して出力される直前のデータをチェックできるので、セキュリティチェック処理のバイパスや、セキュリティチェック開放後の表示データの解読等を極めて困難とする事が可能である。

産業上の利用可能性

10 以上実施例にしたがい説明したように、本発明は、ゲームカートリッジ 2 に記憶された表示データをゲーム機本体 1 に送り、且つこの表示データを前記ゲームカートリッジ 2 に記憶されたゲームプログラムの制御の下にゲーム機本体 1 と接続される表示装置 3 に表示を行うよう
15 している。

したがって、かかる表示データの表示の有無、表示される表示データの内容からゲームカートリッジ 2 及びそこに記憶されるゲームプログラムの真偽性を容易に判断することが出来る。

20 同時に、本発明にしたがいゲーム機本体 1 において、ゲームプログラムの実行中（ゲームの実行中）に繰り返して、ゲームカートリッジ 2 に記憶される表示データと比較基準データとを比較することにより、例えセキュリティチェックの過程を故意的にバイパスするように修正
25 される場合であっても、確実にゲームプログラムの真偽

性を容易に判断できる。

且つ真正でないと判断される場合は、ゲーム機本体 1 の CPU 10 の動作を強制的に止め、以降真正でないと判断されるゲームプログラムの実行を阻止することが可能である。これにより不法に複写、作成されたプログラムの使用を阻止することが出来る。

尚、上記実施例は、ゲーム機を例としているが本発明は、これら実施例に限定されるものではなく、一般的な情報処理装置本体、外部記憶装置及び表示装置を有するものであれば、本発明が適用可能である。

更に、本発明と目的、効果を同じにする均等物も、本発明の保護の範囲に含まれるものである。

請 求 の 範 囲

1. プログラム及び出力データが記憶された外部記憶装置と、

該外部記憶装置が着脱自在に接続され、

5 該外部記憶装置から読み込んだプログラムを実行するCPUと、

基準比較データを記憶する内部記憶装置と、

該外部記憶手段から読み込んだ出力データと該基準比較データとを比較し、これらが不一致の場合にエラー処

10 理信号を発するセキュリティチェック装置とを含む情報処理装置本体及び

該情報処理装置本体が該外部記憶装置から該読み込んだ出力データを表示する表示装置を

有して構成されることを特徴とするセキュリティチェッ

15 ク機能を有する情報処理装置。

2. 請求項1において、前記出力データは、該出力データの
前記出力装置への表示が正当な権原を有しない者の
使用を禁止するものであることを特徴とする情報処理装
置。

20 3. 請求項1又は2において、更に

前記基準比較データと比較される出力データを格納する
出力データ格納装置を有し、該出力データは前記外部
記憶装置に記憶されたプログラムに従って、該外部記憶
装置から該出力データ格納装置に転送され格納されるも

25 のであることを特徴とする情報処理装置。



4. 請求項 1、2 又は 3 において、

前記セキュリティチェック装置は、前記 CPU の動作中に、前記出力データと基準比較データとの比較を繰り返して行うものであることを特徴とする情報処理装置。

5. 請求項 3 又は 4 において、

前記出力データは、前記セキュリティチェック装置によるデータ比較が行われる前に前記外部記憶装置から前記出力データ格納装置に転送記憶され、該セキュリティチェック装置によるデータ比較及び前記出力装置による
10 出力表示の後、該出力データ格納装置から消去されるものであることを特徴とする情報処理装置。

6. プログラム及び出力データが記憶された外部記憶装置から該プログラム及び該出力データを読み込む第一のステップと、

15 該外部記憶装置から読み込んだ該プログラムに含まれる表示チェック開始命令に基づき、チェック開始信号を出力する第二のステップと、

該チェック開始信号が出力される時、該外部記憶装置から読み込んだ出力データと基準比較データとを比較し
20 、これらが不一致の場合にエラー処理信号を発する第三のステップと、

該エラー処理信号に基づき、該プログラムの少なくとも一部の実行を阻止する第四のステップを有することを特徴とする情報処理装置におけるプログラムのセキュリティ
25 チェック方法。



7. 請求項 6 に記載のセキュリティチェック方法において、

前記第三のステップにより、前記出力データと基準比較データとが一致する時に、前記出力データを表示する
5 制御信号を発生し、更に、該制御信号に基づき該出力データを表示する第五のステップを有することを特徴とする情報処理装置におけるプログラムのセキュリティチェック方法。

8. 請求項 6 又は 7 に記載のセキュリティチェック方法
10 において、

前記第一のステップにより、前記外部記憶装置に記憶される出力データを、前記プログラムに従って、読み込むことを特徴とする情報処理装置におけるプログラムのセキュリティチェック方法。

15 9. 請求項 6、7 又は 8 に記載のセキュリティチェック方法において、

前記第三のステップにより、前記出力データと基準比較データとの比較が前記プログラムの実行中に繰り返されることを特徴とする情報処理装置におけるプログラム
20 のセキュリティチェック方法。

10. 請求項 8 又は 9 に記載のセキュリティチェック方法において、更に

前記第五のステップによる出力データの表示の後に、読み込んだ該出力データを消去する第六のステップを有
25 することを特徴とする情報処理装置におけるプログラム



のセキュリティチェック方法。

1 1. 情報処理装置本体に着脱自在に接続される外部記憶装置であって、該情報処理装置本体において実行されるプログラムと、該情報処理装置本体により表示制御される出力データが格納され、該出力データは該プログラムに従って、該情報処理装置への読み込みが制御されることを特徴とする外部記憶装置。

1 2. 請求項 1 1 に記載の外部記憶装置において、

前記情報処理装置は、ビデオゲーム装置であって、前記出力データは、該出力データの表示自体が、前記プログラムの使用権原のない者の違法を意味するものであることを特徴とする外部記憶装置。

1 3. 請求項 1 2 に記載の外部記憶装置において、

前記出力データが前記プログラムの使用権原を与えるものの所有する商標であることを特徴とする外部記憶装置。

1 4. 請求項 1 1 に記載の外部記憶装置において、

前記情報処理装置は、ビデオゲーム装置であって、前記出力データは、前記プログラムにしたがって、該ビデオゲーム実行過程において、所定の時点毎に表示されるように制御されることを特徴とする外部記憶装置。

1 5. 第一のビデオ信号と該第一のビデオ信号より高い表示優先度を有する第二のビデオ信号の表示を制御するビデオ信号制御装置であって、

25 該第二のビデオ信号の表示データと比較されるべき基



準表示データを格納する読出専用メモリと、

該第二のビデオ信号の表示データと該読出専用メモリから読みだされる基準表示データを比較する比較回路と

- 5 該比較回路が該第二のビデオ信号の表示データと該基準表示データとの不一致を検出する時、所定時間後に該第一のビデオ信号の表示を禁止するように制御する回路を有することを特徴とするビデオ信号制御装置。

16. 請求項15において、更に、

- 10 前記第二のビデオ信号の表示期間が観察者により認識可能の時間であるように制御する回路を有することを特徴とするビデオ信号制御装置。

17. 請求項15において、

- 15 前記第二のビデオ信号の表示データは、ビットマップパターンの所定のセキュリティカーソルと、該セキュリティカーソルの表示位置を指定するデータを含み、

前記比較回路は、該セキュリティカーソルの表示位置を指定するデータと、前記基準表示データに含まれる基準表示位置を指定するデータとを比較し、

- 20 該セキュリティカーソルの表示位置が該基準表示位置の範囲内でない時は、前記所定時間後に前記第一のビデオ信号の表示を禁止するように制御する回路により該第一のビデオ信号の表示を禁止することを特徴とするビデオ信号制御装置。

- 25 18. 請求項17において、



前記ビットマップパターンは、観察者に観察可能の固定の大きさで前記第二の表示データが表示されるように前記読出専用メモリに記憶されることを特徴とするビデオ信号制御装置。

5 19. 請求項 17 において、

前記ビットマップパターンの所定のセキュリティカーソルを、特定のロゴマークとしたことを特徴とするビデオ信号制御装置。

