

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2004年4月1日 (01.04.2004)

PCT

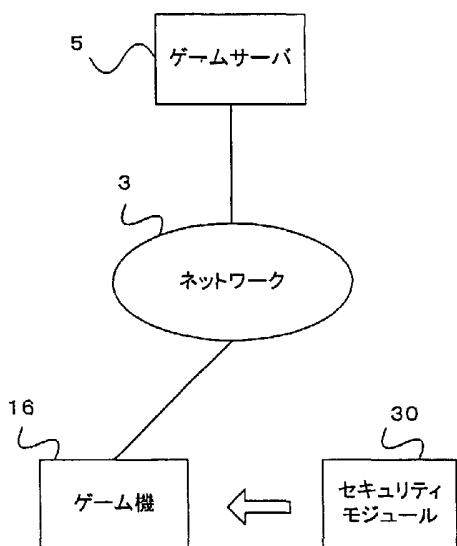
(10) 国際公開番号  
WO 2004/027631 A1

- (51) 国際特許分類: G06F 15/00, (74) 代理人: 中村 聡延 (NAKAMURA, Toshinobu); 〒104-0031 東京都中央区京橋一丁目16番10号オークビル京橋4階東京セントラル特許事務所内 Tokyo (JP).
- H04L 9/32, A63F 13/12, 9/00
- (21) 国際出願番号: PCT/JP2003/011719
- (22) 国際出願日: 2003年9月12日 (12.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
  - 特願2002-272794 2002年9月19日 (19.09.2002) JP
  - 特願2002-356515 2002年12月9日 (09.12.2002) JP
- (71) 出願人: コナミ株式会社 (KONAMI CORPORATION) [JP/JP]; 〒100-6330 東京都千代田区丸の内2丁目4番1号 Tokyo (JP).
- (72) 発明者: 森 昌二 (MORI, Shoji); 〒108-0014 東京都港区芝四丁目1番23号 株式会社コナミコンピュータエンタテインメントスタジオ内 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[ 続葉有 ]

(54) Title: AUTHENTICATION HARDWARE, AUTHENTICATION SYSTEM, AND USE MANAGEMENT HARDWARE

(54) 発明の名称: 認証処理ハードウェア、認証処理システム、及び、利用管理ハードウェア



- 5...GAME SERVER
- 3...NETWORK
- 16...GAME DEVICE
- 30...SECURITY MODULE

(57) Abstract: Authentication hardware is mounted on a game device or the like used for connection with a game server in a network game environment and executes authentication of a user. The authentication hardware includes: a storage section for storing user authentication information; an authentication information transmission section for encrypting authentication information by using an encryption key given from a server device and transmitting the encrypted information to the server device; an authentication result information reception section for receiving authentication result information from the server device; and an authentication result decryption section for decrypting the authentication result information. The authentication information, for example, can include a user ID and a password. The authentication information is stored in the authentication hardware and it is impossible to reference or copy the content from outside of the hardware. Thus, it is possible to assure security of the authentication information. Accordingly, safety can remarkably be improved as compared to the user authentication method in which a user manually inputs a user ID and a password.

(57) 要約: 認証処理ハードウェアは、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などに取り付けられ、ユーザの認証処理を実行する。認証処理ハードウェアは、ユーザの認証情報を記憶する記憶部と、サーバ装置から与えられた暗号鍵で認証情報を暗号化してサーバ装置へ送信する認証情報送信部と、サーバ装置から認証結果情報を受信する認証結果情報受信部と、認証結果情報を復号化する認証結果復号化処理部とを備える。認証情報は、例えばユーザID、パスワードなどを

含むことができる。認証情報は、認証処理ハードウェア内部に記憶されており、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。よって、ユーザがユーザIDやパスワードを手入力するユーザ認証方法と比べて、安全性を大幅に改善することができる。

WO 2004/027631 A1



添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明 細 書

認証処理ハードウェア、認証処理システム、及び、利用管理ハードウェア

## 5 技術分野

本発明は、ネットワークゲームにおけるユーザ認証、利用期間管理などを含むセキュリティ管理手法に関する。

## 背景技術

10 近年では、家庭用ゲーム機などの端末装置でインターネットなどを介してゲームサーバに接続することにより、ユーザがネットワークを利用して各種のゲームを楽しむことができるようになってきている。このようなゲーム環境は広い意味で「ネットワークゲーム環境」などと呼ばれるが、実際にユーザがネットワークを利用する形態は、幾つかのものがある。

15 第1の形態は、ユーザがオンラインでゲームを実行する形態である。即ち、ユーザは、ゲーム機を使用してゲームサーバとの通信を継続した状態でゲーム進行に要するデータをゲームサーバとの間で通信し、ゲームを実行する。この形態では、通常、ユーザがゲームサーバに接続してゲームを開始するたびに、ユーザの  
20 認証処理が要求される。つまり、ゲームサーバにアクセスしたユーザが、ユーザ登録などを完了した登録ユーザであるか、又は、実際にゲームサーバにアクセスしているユーザが登録ユーザ本人であるか、などをチェックする。このようなユーザ認証は、一般的にはユーザ登録時に発行されたユーザID及びパスワードを  
25 ユーザがゲーム機に対して入力し、ゲームサーバへ送信することにより行われる。ゲームサーバは、受信したユーザID及びパスワードが登録ユーザのものであるかをチェックし、ユーザ認証を実行する。

一方、第2の形態では、ユーザはオンラインでゲームを実行するのではなく、ゲームプログラムの流通手段としてネットワークを利用する。つまり、ユーザはネットワークを介してゲームサーバへ接続し、所望のゲームを選択してそのゲームプログラムを自分のゲーム機へダウンロードする。ダウンロードが完了すれば

ゲームプログラム自体はユーザのゲーム機側に存在するので、原則としてユーザはゲームを実行するためゲームサーバへ接続する必要はなくなる。

ネットワークを利用したゲームにおいては、幾つかの問題がある。その1つはユーザの認証の問題である。上述のように第1の形態においては、ユーザ認証は一般的にユーザIDとパスワードの組み合わせによって行われる。しかし、ユーザIDとパスワードを利用したユーザ認証処理は、以下のような理由でセキュリティ面では非常に弱いと言わざるをえない。

まず、ユーザIDやパスワードは第三者による複製、偽造が容易である。ユーザIDやパスワードは単なる文字列であり、しかもユーザがゲーム機に対して手入力することを前提に作成されているため、せいぜい10桁程度の長さであるのが普通である。よって、不正に他の登録ユーザになりすましてゲームを行おうとする者は、何通りもの文字列を推測して入力することにより、比較的容易に他人のユーザIDやパスワードを推測することができる。また、一旦他人に知られると、さらに他の者へと急速に頒布される危険性もある。1つのユーザID及びパスワードを複数人が同時に使用できるので、ユーザIDやパスワードが広まってしまうと、誰もがそれを利用して不正にゲームを行うことができってしまう。

ユーザIDやパスワードの桁数を増やせば推測は困難となるのであるが、一般的にユーザIDやパスワードは人間が記憶しておき手入力するものであるから、入力間違いやパスワードの紛失（忘れる）が起きやすい。よって、結局それほど長いユーザIDやパスワードを使用することはできず、安全性の面では自ずと限界がある。

さらには、ユーザがゲーム機からゲームサーバへ送信したユーザIDやパスワードを、ネットワーク上の通信途中において傍受して取得したり、ダミーの認証サーバを構成してゲーム機に対してあたかもユーザ認証が成功したかのように認証結果情報を送信して、不正にゲームを実行可能とすることも可能である。

一方、上述の第2の形態のように、ネットワークをゲームプログラムの流通手段として使用する場合には、ユーザに対するゲームの使用期限管理の問題がある。通常、ユーザがダウンロードするゲームプログラムは有料であり、使用料の支払いを条件に一定期間（無期限の場合を含む）ゲームの使用を許可する方式が一般

的である。このような場合に、使用期間を管理するために行われる1つの方法は、ユーザがゲームを始める際に、まずゲームサーバへ接続して認証処理を行うことを義務づける方法である。ゲームサーバは、ユーザから接続があると、そのユーザのゲームの使用期限をチェックし、使用期限内である場合にはゲームの実行を  
5 許可する情報をゲーム機へ送信してゲームを実行可能とする。

しかし、ゲームを開始するたびにゲームサーバへの接続が要求されるというのは、ユーザにとっては煩雑であり、また、通信コストもかかる。よって、使用料の支払いが完了すれば、ユーザにゲームサーバへの接続を行わせることなく、ゲーム機側のみで利用可能な期間を管理することが望まれる。

10

#### 発明の開示

本発明の目的は、以上の点に鑑みてなされたものであり、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、ユーザの認証や使用期限の管理を確実にを行い、ユーザが安全かつ快適にゲームを行うことを可能  
15 とすることにある。

本発明の1つの観点では、ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証  
20 処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部と、受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理  
25 部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備える。

上記のハードウェアは、端末装置に取り付けられることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ

装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザID、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

10 暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報  
15 に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止できる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与え  
20 られ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

なお、暗号化処理部、送信部、受信部及び復号化処理部は、集積回路として構成することができ、これにより各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる。

また、記憶部は取り外し可能に構成することができる。これにより、ハードウェアの他の部分を故障その他の理由により交換する必要が生じた場合に、認証情報を記憶した記憶部のみは交換せず、そのまま使用し続けることができる。よって、認証情報を変更する必要なく、ハードウェアの交換やバージョンアップなどに対応することができる。

上記の認証処理ハードウェアの一態様では、前記復号化処理部は、1つの前記

暗号鍵を利用した復号化処理を1回に限り行う。これにより、サーバ装置から送信された暗号化済みの認証結果情報をネットワーク上で取得し、ダミーの認証サーバなどを利用して端末装置へ送信した場合でも、その暗号化済み認証結果情報に対応する暗号鍵は既に使用済みとなっているため、認証結果情報の復号化は行  
5 えない。これにより、ダミーの認証サーバなどを利用した不正な認証処理を防止することができる。

上記の認証処理ハードウェアの他の一態様は、前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備える。これにより、認証結果に応じて端末装置を動作させることができる。

10 本発明の他の観点では、ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアと、を備える認証処理システムが提供される。前記サーバ装置は、前記ハードウェアからの認証要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する  
15 暗号鍵送信部と、前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備える。また、前記ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、受信した前記暗号鍵を利用して前記認証情報を  
20 を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴  
25 う処理の実行許可を与える実行許可部と、を備える。また、前記端末装置は、前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備える。

上記の認証処理システムによれば、ハードウェアは、端末装置に取り付けられ

ることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザID、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止できる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与えられ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

本発明の他の観点では、端末装置に取り付けられ、前記端末装置の利用期限管理処理を実行する期限管理ハードウェアは、前記端末装置の利用期限を示す利用期限情報を記憶する記憶部と、前記端末装置から、動作要求を受信する受信部と、時計部と、前記時計部を利用して、前記動作要求を受信した時点が前記利用期限情報が示す利用期限を経過しているか否かを判定する判定部と、前記動作要求を受信した時点が前記利用期限を経過していないと前記判定手段が判定したときに、前記端末装置を動作可能とする制御部と、を備える。

上記のハードウェアは、端末装置の利用期限の管理を行う。記憶部内には、端



末装置の利用期限情報が記憶されている。端末装置から動作要求がなされると、時計部の時計機能を利用し、現在の時点において利用期限を過ぎているか否かが判定される。利用期限内であれば、端末装置の動作を許可する。これにより、利用期限の管理を容易に行うことができる。

- 5      なお、受信部、時計部、判定部及び制御部は、集積回路として構成することができる。これにより、各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる。

#### 図面の簡単な説明

- 10      図 1 は、本発明を適用したネットワークゲーム環境の概略構成を示すブロック図である。
- 図 2 は、ゲーム装置の概略構成を示すブロック図である。
- 図 3 は、セキュリティモジュールの内部構成を示す機能ブロック図である。
- 図 4 は、ユーザ認証処理のフローチャートである。
- 15      図 5 は、使用期限管理処理のフローチャートである。
- 図 6 は、本発明の変形例によるゲーム機とセキュリティモジュールの構成を示すブロック図である。

#### 発明を実施するための最良の形態

- 20      以下、図面を参照して本発明の好適な実施の形態について説明する。

##### [ネットワークゲーム環境]

- 図 1 に本発明を適用したネットワークゲーム環境の概略構成を示す。図 1 において、ゲームの提供者が運営するゲームサーバ 5 と、ユーザが使用するゲーム機 16 とがネットワーク 3 を介して通信可能に構成されている。ネットワーク 3 の
- 25      1 つの好適な例はインターネットであるが、それ以外のネットワークであってもよい。また、ネットワーク 3 がインターネットである場合には、ユーザのゲーム機 16 とネットワーク 3 との間にはインターネットサービスプロバイダ (ISP) その他が介在することとなるが、ここではそれらの説明は省略する。

        ゲーム機 16 は、好適にはユーザが家庭で使用するゲーム機であるが、遊技場

などに設置される業務用のゲーム機であっても構わない。なお、図1においては説明の便宜上、1台のゲーム機16のみが図示されているが、実際には多数のユーザが所有する多数のゲーム機16が同様にネットワーク3を介してゲームサーバ5と通信可能に構成される。

5     ゲームサーバ5は、ユーザに対してネットワーク3を通じてゲームを提供する。ゲーム提供の1つの形態は、前述のようにゲーム機16とゲームサーバ5との間で通信することにより、ユーザがオンラインでゲームを実行するものである。この場合、ゲームサーバ5とユーザとが1対1でゲームを実行する場合もあるし、  
10     ゲームサーバ5の管理下で複数のユーザが各々ゲーム機16を操作して同時に同一のゲームを実行する場合もある。いずれの場合にも、ユーザは、ゲームを開始するときにはゲームサーバ5へ接続し、ユーザ認証処理を行うことになる。

一方、前述の第2の形態では、ユーザはネットワークを1つの流通手段として利用し、ゲームサーバ5から所望のゲームプログラムをダウンロードする。ゲームプログラムは通常は有料であり、ユーザはゲームプログラム使用料を、何らかの方法でゲームサーバ5を運営する会社に対して支払う。ゲームプログラム使用料の支払いにより、ユーザは所定期間のゲーム使用权を取得することになる。ゲームサーバ5は、ユーザによるゲームプログラム使用料の支払いを条件に、ネットワーク3を通じてゲームプログラムをユーザのゲーム機16へダウンロードさせる。その後は、ユーザは、既に支払ったゲームプログラム使用权の範囲内（例えば、所定期間内）では、ダウンロードしたゲームプログラムを自由に使用することができる。よって、ゲームサーバ5を運営するゲーム提供者は、使用期限が経過したときにユーザによる当該プログラムの使用を禁止するための方策を採る必要がある。以下、この処理を「使用期限管理」と呼ぶことにする。

25     図1に示すように、本発明のネットワークゲーム環境では、セキュリティモジュール30が使用される。セキュリティモジュール30は、上述のユーザ認証や使用期限管理を行うために使用される専用モジュールであり、ゲーム機16に取り付けて使用される。物理的にはセキュリティモジュール30は内部構造がわからないように製作されたハードウェア装置であり、ゲーム機16の所定のコネクタなどに取り付けられる。ゲーム機16は、セキュリティモジュール30が取り

付けられた状態でなければ、ゲームサーバ5を利用したネットワークゲームを実行できないように構成される。なお、ゲームサーバ5とは無関係の市販ゲームソフトなどを使用する場合には、ゲーム機16はセキュリティモジュール30なしでも動作するように構成することができる。本発明では、セキュリティモジュール30を使用することにより、前述のユーザ認証処理や使用期限管理などを、簡単かつ確実に実行することが可能となる。

[ゲーム機の構成]

次に、図1に示すゲーム機の構成について説明する。図2はゲーム機16を含むゲーム装置20のブロック図である。

10 このゲーム装置20は、モニタ9、スピーカ10a及び10b、コントローラ12、補助記憶装置13、DVD-ROM15、ゲーム機16で構成される。モニタ9には家庭用のテレビ受像機が、スピーカ10a及び10bにはそのテレビ受像機の内蔵スピーカが一般に使用される。スピーカは、右チャンネルスピーカ10a及び左チャンネルスピーカ10bの2チャンネルを有する。コントローラ12は入力装置として機能するものであり、そこにはプレイヤーによる操作を受け付ける操作部材が設けられる。補助記憶装置13は、ゲーム進行状況などに関連するデータを記憶するための記憶媒体であり、例えば半導体メモリなどを使用することができる。

20 ゲーム機16は、マイクロプロセッサを主体として構成されたCPU1と、そのCPU1に対する主記憶装置としてのROM2及びRAM3と、画像処理及び音声処理用のグラフィックスプロセッシングユニット(GPU)4及びサウンドプロセッシングユニット(SPU)6と、それらのユニットに対するバッファ5、7と、DVD-ROM読取装置8と、インターフェース17と、コネクタ18と、ハードディスク(HDD)19と、を有している。

25 ROM2には、ゲーム機の動作制御に必要なプログラムとしてのオペレーティングシステムが格納されている。RAM3には記憶媒体としてのDVD-ROM15から読み取ったゲーム用のプログラムやデータが必要に応じて書き込まれる。

GPU4はCPU1から画像データを受け取ってフレームバッファ5上にゲーム画面を描画するとともに、その描画された画像のデータを所定のビデオ再生信

号に変換して所定のタイミングでモニタ 9 に出力する。S P U 6 は、D V D - R O M 1 5 から読み出されてサウンドバッファ 7 に記録された音声、楽音等のゲーム音データ等を再生してスピーカから出力させる。

D V D - R O M 読取装置 8 は、C P U 1 からの指示に従って D V D - R O M 1 5 上に記録されたプログラムやデータを読み取り、その読み取った内容に対応した信号を出力する。H D D 1 9 には、ゲームサーバ 5 からダウンロードしたゲームプログラムなどが格納される。

コネクタ 1 8 は、セキュリティモジュール 3 0 をゲーム機 1 6 に取り付ける際に使用され、セキュリティモジュール 3 0 側のコネクタと接続される。コネクタ 1 8 は、インターフェース 1 7 を介してバス 1 4 と接続されている。

C P U 1 にはバス 1 4 を介して通信制御デバイス 1 1 が接続され、通信制御デバイス 1 1 にはコントローラ 1 2 及び補助記憶装置 1 3 がそれぞれ着脱自在に接続される。通信制御デバイス 1 1 は一定周期（例えば 1 / 6 0 秒）でコントローラ 1 2 の操作部材の操作状態を走査し、その走査結果に対応した信号を C P U 1 15 に出力する。C P U 1 はその信号に基づいてコントローラ 1 2 の操作状態を判別する。また、通信制御デバイス 1 1 は、ネットワーク 3 を介してゲームサーバ 5 と必要な通信を行うために機能する。

ゲーム機 1 6 は、記憶媒体としての D V D - R O M 1 5 に記録されたゲームプログラムに従って所定のゲームを実行することができる。また、ネットワーク 3 20 をゲームプログラムのダウンロード手段として使用する場合には、ゲームサーバ 5 からダウンロードしたゲームプログラムは、ゲーム機 1 6 内部の H D D 1 9 に保存される。よって、ゲーム機 1 6 は、D V D - R O M 1 5 に記録されたゲームプログラムの代わりに、ゲームサーバ 5 からダウンロードし、H D D 1 9 に格納したゲームプログラムに従ってゲームを実行することもできる。

ネットワークゲーム実行時には、C P U 1 は、D V D - R O M 1 5 に記録されたゲームプログラム又はゲームサーバ 5 からダウンロードしたゲームプログラムを実行する。そして、その過程で発生する、ゲーム機 1 6 におけるユーザのプレイ状況データを、通信制御デバイス 1 1 及びネットワーク 3 を介してゲームサーバ 5 に送信する。また、必要に応じて、サーバが生成するゲーム状況データや、

ネットワーク上で同時にゲームをプレイしている他のユーザのプレイ状況データをゲームサーバ5から受信する。こうして、ゲーム機16はオンラインゲームを進行させる。

[セキュリティモジュール]

5 次に、セキュリティモジュールについて説明する。図3にセキュリティモジュール30の概略構成を示す。図3に示すように、セキュリティモジュール30は、大別すると、I/Fユニット30a、処理ユニット30b及び記憶ユニット30cにより構成される。セキュリティモジュール30内部の各ユニットはメモリ、フラッシュ、及び集積回路などを含むハードウェアユニットとして、内部に記憶  
10 した情報に対する外部からのアクセスが不能となるように構成される。これは、例えばゲーム機16への取付用コネクタ40などのゲーム機16との入出力手段を除き、外部からの入出力手段や入出力端子を設けないなどの方法で実現できる。

I/Fユニット30は、ゲーム機16との接続のためのユニットであり、I/F31と、コネクタ40とを備える。コネクタ40は、図2に示すゲーム機16  
15 のコネクタ18と接続される。I/F31は、セキュリティモジュール30内のデータとゲーム機16側のデータとの間のインターフェース処理を行う。

記憶ユニット30cは、認証情報記憶部38と、不揮発性メモリ39とを備える。認証情報記憶部38は、ユーザID、パスワードなどの認証情報を記憶する。一方、不揮発性メモリ39は、認証情報以外の各種情報を記憶する。具体的には、  
20 ユーザが特定の有料ゲームプログラムをダウンロードした場合の使用期限情報を記憶する。使用期限情報は、例えば「〇年〇月〇日」のように終了日時で記憶してもよく、何百時間というように時間で記憶しても良い。

処理ユニット30bは、CPUなどにより構成され、時計機能33、暗号化機能34、復号化機能35及び通信機能36を備える。CPUが予め用意された各  
25 プログラムを実行することにより、各機能が実現される。時計機能33は、セキュリティモジュール独自の内部時計であり、基本的に外部からの調整などができないように構成される。

暗号化機能34は、ユーザ認証処理において、認証情報記憶部38に記憶されている認証情報（ユーザID、パスワードなど）を所定の暗号鍵を利用して暗号

化する処理を行う。暗号化された認証情報は、ユーザ認証処理においてゲームサーバ5へ送られる。復号化機能35は、ゲームサーバ5から送信された暗号化済み情報を復号化する。また、通信機能36は、暗号化されたユーザ認証情報やゲームサーバから送信される情報などの通信処理を実行する。

5 [ユーザ認証処理]

次に、ユーザ認証処理について説明する。ユーザ認証処理は、ユーザがゲーム装置20を使用してゲームサーバ5に接続し、ネットワークゲームを開始する際に実行される処理であり、当該ユーザがゲームをプレイすることができる登録ユーザであるか否かを判別するための処理である。

- 10 通常、ユーザ認証処理においては、ユーザ自身がユーザIDやパスワードなどの認証情報をゲーム装置20対して入力し、それがネットワーク3を介してゲームサーバ5へ送信される。これに対し、本発明では、ユーザID及びパスワードなどの認証情報はセキュリティユニット30の認証情報記憶部38内に記憶されており、外部からアクセスすることはできない。即ち、認証情報はハードウェア
- 15 の形態でセキュリティモジュール30に実装されているので、複製が困難であり、また、記憶されている認証情報をセキュリティモジュール30から外部へ取り出すことも困難である。また、ユーザ自身も、実際に記憶されている認証情報を知らなくても、セキュリティモジュール30を所持していれば済むので、認証情報
- 20 自体が漏洩したり、不正に流通することが防止できる。また、万が一第三者が認証情報を知得することができたとしても、その認証情報をユーザ認証処理において入力する術がない。また、セキュリティモジュール30は物理的な1つの存在
- であるため、複数人間が同時に使用することはできない。さらに、人間がユーザIDやパスワードを手入力する場合と異なり、入力ミスも発生しないし、ユーザIDやパスワードの桁数をかなり長くすることができるので安全性をより高め
- 25 ることができる。

次に、セキュリティモジュール30とゲームサーバ5との間で行われるユーザ認証処理について説明する。なお、セキュリティモジュール30から入出力されるデータは、まずゲーム機16に入力されることになるが、ゲーム機16内を単に通過するだけであり、ゲーム機16はそのデータに対して特に処理を行わない。

つまり、ユーザ認証処理は実質的にセキュリティモジュール30とゲームサーバ5との間で実行されることになる。

ユーザ認証処理においては、セキュリティモジュール30内に記憶されているユーザの認証情報（ユーザID、パスワードなど）を、ネットワーク3を介して  
5 ゲームサーバ5へ正しく送信することが要求される。また、その際に、第三者が送信されたデータをネットワーク上で不正に傍受し、認証情報を知得することを防止しなければならない。このため、本実施形態では、セキュリティモジュール30は、暗号化機能34により認証情報を暗号化してからゲームサーバ5へ送出する。これにより、第三者がネットワーク3上で送信されたデータを取得し、  
10 それから認証情報を解析することが防止できる。

また、ゲームサーバ5上で登録ユーザに対するユーザ認証が正しく完了すると、ゲームサーバ5はその旨の通知、つまり、当該ユーザのゲーム機16にゲームの実行を許可するための許可情報をセキュリティモジュール30へ送信することになる。セキュリティモジュール30は、この許可情報を受け取ると、ゲーム機1  
15 6を制御してゲームの実行を可能とする。ゲームサーバ5はこの許可情報も暗号化して送出する。

一方、ユーザのゲーム使用期間が終了した場合、当該ユーザは同様の手順でゲームサーバ5へユーザ認証を行っても、ゲームサーバ5側は当該ユーザのゲーム使用期間が終了したことを知っているため、ユーザ認証は不成功に終わる。

20 そのような場合、当該ユーザは、ゲーム使用期間満了前に正しくユーザ認証処理が行われた際にゲームサーバ5からセキュリティモジュール30へ送信された許可情報をネットワーク3上で取得しておき、ゲーム使用期間の終了後にダミーサーバ（偽りのゲームサーバとして機能する）を用意して、同じ許可情報をダミーサーバから自己のゲーム機16へ送信しようとすることがありうる。こうすると、ゲーム機16は、ダミーサーバからの許可情報をゲームサーバ5からの許可  
25 情報であると誤認し、ゲームを実行してしまう可能性がある。

このような不正なユーザ認証を防止するために、本実施形態では、ゲームサーバ5からセキュリティモジュール30へ送信される許可情報（暗号化済み）を1回限り有効とする。即ち、1つの許可情報は、セキュリティモジュール30上に

において一回のみ有効であるとする。これは、例えばセキュリティモジュール30内に、過去にゲームサーバ5から受信した許可情報の履歴を保存しておき、過去に使用された許可情報と同一の許可情報を再度受け取っても、その許可情報を無効とし、ゲームの実行を許可しないようにすることにより実現することができる。

5       また、許可情報を1回限り有効とする代わりに、許可情報を暗号化する鍵を1回限り有効とする方法もある。即ち、ゲームサーバ5は、特定の暗号鍵を使用して許可情報を暗号化し、セキュリティモジュール30へ送信する。セキュリティモジュール30は、その暗号鍵をゲームサーバ5から取得しており、当該暗号鍵を使用して許可情報を復号化し、ゲームを実行可能とする。ここで、セキュリティモジュール30内では、一度使用された暗号鍵はその後の許可情報の復号化処理には使用できないように構成しておく。こうすれば、前述のダミーサーバから過去に使用した暗号鍵で暗号化された許可情報をゲーム機16に再度送って不正にゲームを実行しようとした場合でも、その暗号鍵は既に過去に使用履歴があり、再度使用することはできないので、セキュリティモジュール30は許可情報を得ることができない。これにより、使用期間経過後などの不正なゲーム実行を防止  
10       することができる。

次に、ユーザ認証処理の具体例について図4を参照して説明する。図4は、ユーザ認証処理のフローチャートである。まず、セキュリティモジュール30は、ゲームサーバ5へ接続し、ユーザ認証を行う旨を要求する(ステップS1)。ゲームサーバ5は、これに対して、所定の暗号鍵を作成し、セキュリティモジュール30へ送信する(ステップS2)。なお、暗号鍵は、セキュリティモジュール30とゲームサーバ5との間で認証情報や許可情報を送受信する際の暗号化及び復号化に使用される鍵であり、例えば乱数などとすることもできる。  
20

セキュリティモジュール30は、暗号鍵を受信すると、認証情報記憶部38から認証情報を取得し、これを暗号鍵で暗号化することにより暗号化した認証情報を作成してゲームサーバ5へ送信する(ステップS3)。認証情報は、例えばユーザID、パスワードなどを含む。ゲームサーバ5は、暗号化した認証情報を受信し、暗号鍵を使用して復号化することにより、認証情報を取得する(ステップS4)。そして、ゲームサーバ5は、認証情報が登録ユーザのものであるか否か  
25



を判定する（ステップS5）。これは、例えば登録ユーザについてのユーザ情報を記憶したデータベースなどを参照して、受信した認証情報が正規な登録ユーザのものであるか否かを判定することにより行われる。

認証情報が正規な登録ユーザのものであった場合（ステップS5；Yes）、ゲームサーバ5はゲーム実行許可情報を生成し、これを暗号鍵で暗号化して暗号化済み許可情報を作成する（ステップS6）。一方、認証情報が正規な登録ユーザのものでなかった場合（ステップS5；No）、ゲームサーバ5は所定のエラー処理を行い、ダミーデータを作成する（ステップS7）。ここで、ダミーデータは、不正な目的によりデータの解析が行われることを防止するために生成されるものであり、例えば全く無意味なデータとすることができる。そして、ゲームサーバ5は、ステップS6で生成された暗号化済み許可情報又はステップS7で生成されたダミーデータを、認証結果情報としてセキュリティモジュール30へ送信する（ステップS8）。

セキュリティモジュール30は、認証結果情報を受信すると、暗号鍵でこれを復号化し（ステップS9）、ゲーム実行が許可されたか否かを判定する（ステップS10）。認証結果情報が暗号化済み許可情報である場合、ステップS9の復号化処理により、暗号化が解除された許可情報が得られる。よって、セキュリティモジュール30は、ゲーム装置20に対してゲーム実行を許可し、ゲームを実行させる（ステップS11）。一方、認証結果情報がダミーデータである場合、ステップS9の復号化は正しく行うことができないので、セキュリティモジュール30はゲームの実行が許可されていないと判断し、ゲーム装置20に対してゲームの実行許可を与えない（ステップS12）。

以上のようにして、暗号鍵を使用して暗号化した認証情報及び許可情報を通信することにより、ユーザ認証がなされる。ゲームサーバ5は、セキュリティモジュール30からユーザ認証の要求を受けるたびに、新しい暗号鍵を作成し、セキュリティモジュール30へ送信する。従って、ステップS6で生成される許可情報は必ず新しい暗号鍵により暗号化されていることになり、セキュリティモジュール30は新しい暗号鍵を有する正当な登録ユーザでなければゲーム実行を可能とする許可情報を取得することができない。

また、セキュリティモジュール30は、一度ゲームサーバから受信した暗号鍵を1回限り使用し、繰り返し使用しないこととする。これは、例えば、ユーザ認証要求を行うたびに、その後のステップS3でゲームサーバ5から受信した暗号鍵のみを使用するようにプログラムを構成するとか、一度ステップS9の復号化  
5 処理で使用した暗号鍵を消去するなど、いくつかの方法で実現することができる。

この方法によれば、前述のダミーサーバを利用した不正な認証処理も不成功とさせることができる。例えばあるユーザがプログラム使用期限の終了などにより正当にゲームを実行できなくなった状態で、前述のダミーサーバを用意し、過去にゲームサーバ5から送信された認証結果情報を偽りの認証結果情報としてダミ  
10 ーサーバからセキュリティモジュール30に送信したとする。セキュリティモジュール30はステップS9で認証結果情報を復号化するが、その認証結果情報を正しく復号化できる暗号鍵は過去に既に使用済みであり、セキュリティモジュール30はその暗号鍵を1回のみ使用することとしているので、当該偽りの認証結果情報に基づいてセキュリティモジュール30がゲーム実行許可を発することは  
15 ない。よって、ダミーサーバを利用する不正な認証処理を無力化することができる。

なお、暗号化処理は一般的には特定の関数による演算処理であり、暗号鍵は当該関数の演算処理に使用するパラメータを示すデータとすることができる。

#### [使用期限管理]

20 次に、使用期限管理について説明する。使用期限管理とは、事前にゲーム使用料を支払ってゲームの使用権を得たユーザに対して、使用期限を管理し、使用期間経過後はゲームの使用を禁止するための処理である。このような使用期限管理は、ゲーム使用権を得た後でも、ユーザに対して常にゲーム開始前にゲームサーバ5へ接続してユーザ認証を行うことを義務付ければ、ゲームサーバ側で容易に  
25 行うことができる。しかし、正当な使用期間内であるにも拘わらず、ゲーム開始時にいちいちゲームサーバへ接続して認証処理を行うことは、ユーザにとっては煩雑であったり、不快であったりする。また、ゲームサーバへ接続することにより、通信コストが発生し、ユーザはこれを負担する必要がある。よって、一度ゲームプログラム使用料を支払った後は、ゲームサーバへ接続する必要なく、ゲー

ム機側のみで使用期限の管理ができることが望ましい。本発明では、セキュリティモジュール 30 によりこれを実現する。

具体的には、図 3 に示すセキュリティモジュール 30 の不揮発性メモリ 39 内に、使用期限情報が格納される。使用期限情報は、例えば何年何月何日まで使用可能であるという日時の情報、又は、合計何時間使用可能であるなどの時間情報などの形態で記憶することができる。

また、セキュリティモジュール 30 内部の時計機能 33 は、基本的に外部からの調整ができないように構成される。よって、ユーザがセキュリティモジュール 30 内の時計機能 33 にアクセスし、時刻を調整、変更することはできない。通常、ゲーム機 16 内にも時計機能は内蔵されているが、これはユーザにより容易に変更可能に構成されている。よって、ゲーム機 16 内の時計機能を利用して使用期限を管理するのでは、ユーザによる不正な時刻変更が容易に行われてしまう。この点、本発明のセキュリティモジュール 30 によれば、内部の時計機能 33 は外部からは変更不能であるので、使用期限を正しく管理することができる。

使用期限管理処理の一例を図 5 を参照して説明する。図 5 は、使用期限管理処理のフローチャートである。まず、ユーザが特定のゲームを実行すべくゲーム機 16 を操作すると、ゲーム機 16 はセキュリティモジュール 30 に対してゲーム実行要求を行う（ステップ S 30）。セキュリティモジュール 30 は、ゲーム実行要求を受け取ると、まず不揮発性メモリ 39 から使用期限情報を取得し（ステップ S 31）、次に時計機能 33 を利用して使用期限内であるか否かを判定する（ステップ S 32）。

使用期限を過ぎている場合（ステップ S 33 ; No）、セキュリティモジュール 30 はゲーム機に対してゲーム実行を許可しない（ステップ S 34）。一方、使用期限内である場合（ステップ S 33 ; Yes）、セキュリティモジュール 30 はゲーム機に対してゲーム実行許可を与える。よって、ユーザはゲームを実行することができる。

なお、上記の説明では使用期限管理を日時や時間情報により行う例を示したが、本発明における使用期限管理はそのような時間による管理には限定されない。例えば、使用期限をゲーム何回分などという使用回数として設定し、セキュリティ

モジュール 30 内にカウンタ機能を設けて使用回数をカウントすることにより使用期限を管理することもできる。また、ユーザが複数のゲームを選択的にプレイできる環境では、使用可能なポイント数を予めセキュリティモジュール 30 内に記憶し、ユーザがあるゲームをプレイすると、そのゲームに対応するポイント数  
5 だけセキュリティモジュール 30 内に記憶されたポイント数を減算していくこともできる。この場合のポイント数は、ゲームをプレイするためのプリペイド方式の電子マネー的な意味を有することになる。なお、そのようにセキュリティモジュール内にカウンタ機能を設ける場合には、前述の時計機能と同様に外部からカウント値の調整やリセットなどが不能なようにカウンタ機能を構成する。

10 [変形例]

上記の実施例においては、セキュリティモジュール 30 をゲーム機 16 に取り付け、セキュリティモジュール 30 とゲームサーバ 5 との間のデータ通信はゲーム機 16 内を通過するように構成されていた。代わりに、図 6 に示すように、セキュリティモジュール 30 がネットワーク 3 に接続され、ゲーム機 16 へはセキュリティモジュール 30 内を通過してデータが供給されるように構成することも  
15 できる。この場合、セキュリティモジュール 30 によるユーザ認証の対象となるデータはセキュリティモジュール 30 による処理後にゲーム機 16 に送られる。一方、セキュリティモジュール 30 の処理対象外のデータ（例えば無償のゲームプログラムのダウンロードなど）は、セキュリティモジュール 30 内をそのまま  
20 通過してゲーム機 16 へ送られる。

図 3 に示すように、セキュリティモジュール 30 は I/F ユニット 30 a、処理ユニット 30 b 及び記憶ユニット 30 c により構成されている。ここで、セキュリティモジュール 30 は、3 つのユニットを一体的に構成することもできるが、記憶ユニット 30 c のみを例えばカード型の記憶媒体などとして、他の 2 つの  
25 ユニットから取り外し可能に構成することもできる。これには以下のようなメリットがある。3 つのユニットが一体的に構成されていると、例えば I/F ユニット 30 a 及び処理ユニット 30 b 内のいずれかの箇所が故障したような場合、3 つのユニット全体として交換を行う必要がある。また、故障に限らず、セキュリティモジュール 30 による処理が多機能化したような場合にも、セキュリティモジ

ジュール全体を交換する必要がある。しかし、記憶ユニット30cはユーザの認証情報及びゲームの使用期限情報などの情報を記憶したユニットであるので、これを含めてセキュリティモジュール30全体を交換してしまうと、記憶ユニット30c内に記憶されている認証情報やゲーム使用期限情報などを使用不可となつてしまう。この点、記憶ユニット30cのみを取り外し可能に構成しておけば、上記のような理由で他の2つのユニットを交換する必要がある場合でも、記憶ユニット30c内の認証情報などをそのまま引き継ぐことができる。

以上説明したように、本発明によれば、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、高いセキュリティを確保してユーザが安全かつ快適にゲームを行うことが可能となる。

#### 産業上の利用可能性

本発明は、ネットワークを通じた通信を利用し、ユーザがゲーム機などの端末装置を操作するネットワークゲーム環境におけるユーザの認証処理や利用管理などに利用することができる。

## 請 求 の 範 囲

1. ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証  
5 処理ハードウェアであって、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

10 前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

15 前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備えることを特徴とする認証処理ハードウェア。

2. 前記復号化処理部は、1つの前記暗号鍵を利用した復号化処理を1回に限り行うことを特徴とする請求の範囲第1項に記載の認証処理ハードウェア。  
20

3. 前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備えることを特徴とする請求の範囲第1項又は第2項に記載の認証処理ハードウェア。  
25

4. ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行するハードウェアと、を備える認証処理システムであって、前記サーバ装置は、

前記ハードウェアからの認証要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する暗号鍵送信部と、

前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備え、

5 前記ハードウェアは、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

10 前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

15 前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備え、

前記端末装置は、

20 前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、

前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備えることを特徴とする認証処理システム。

5. 端末装置に取り付けられ、前記端末装置の利用期限管理処理を実行する期限管理ハードウェアであって、

前記端末装置の利用期限を示す利用期限情報を記憶する記憶部と、

前記端末装置から、動作要求を受信する受信部と、

時計部と、

前記時計部を利用して、前記動作要求を受信した時点が前記利用期限情報が示

す利用期限を経過しているか否かを判定する判定部と、

前記動作要求を受信した時点が前記利用期限を経過していないと前記判定手段が判定したときに、前記端末装置を動作可能とする制御部と、を備えることを特徴とする期限管理ハードウェア。



図1

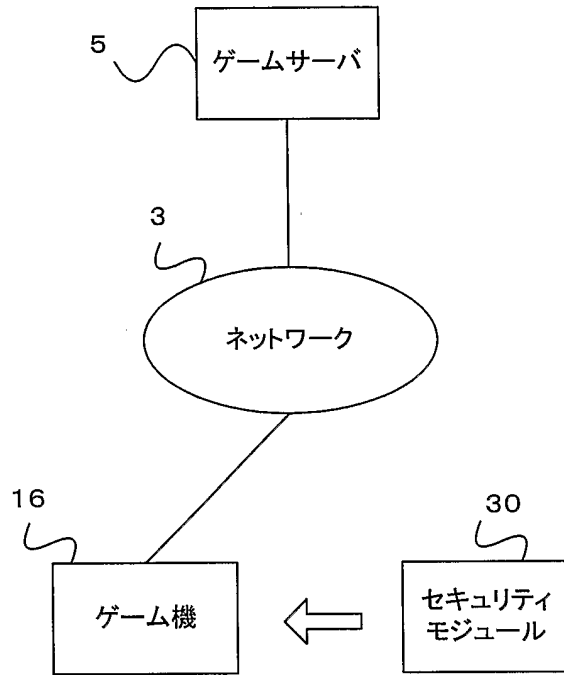


図2

20

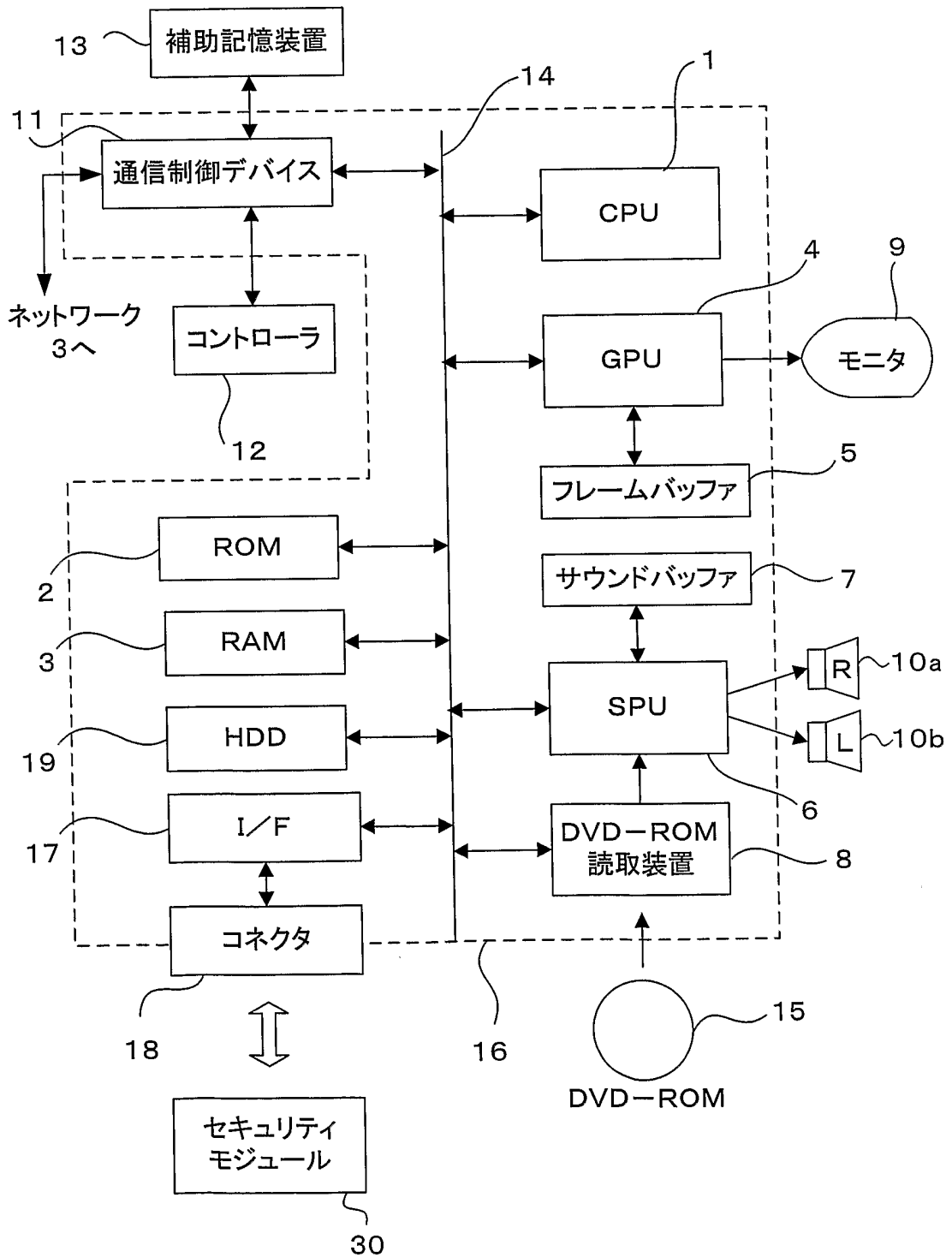


図3

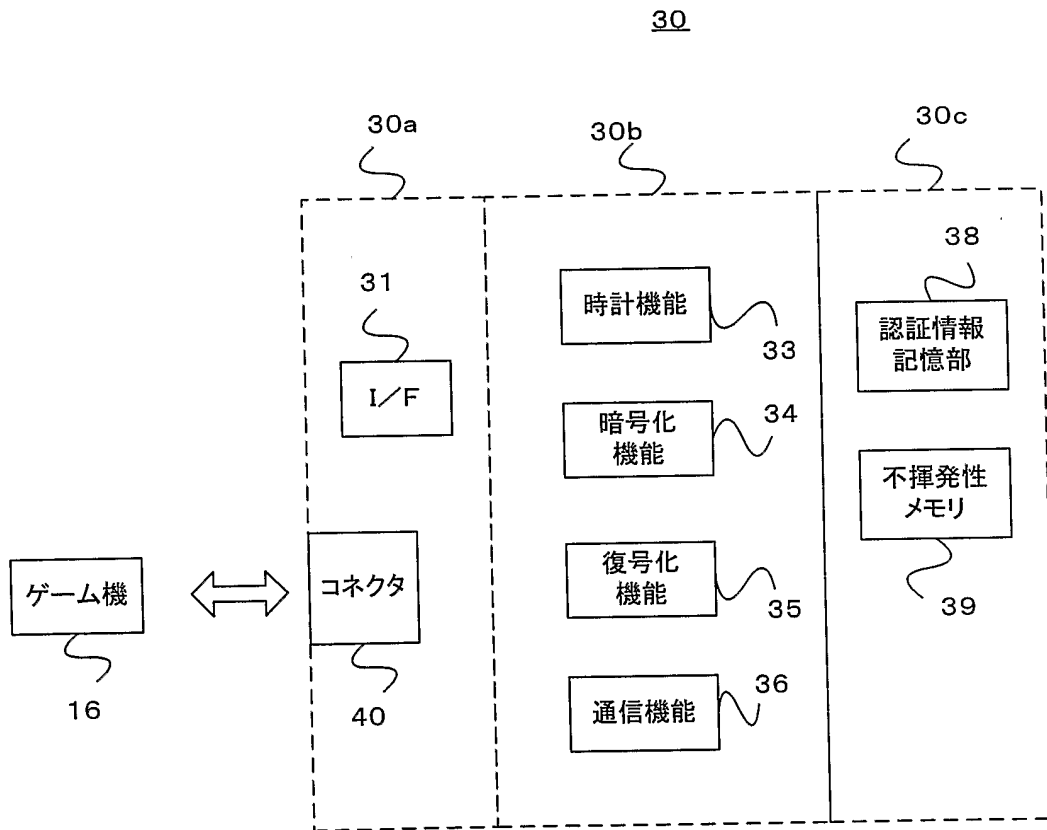


図4

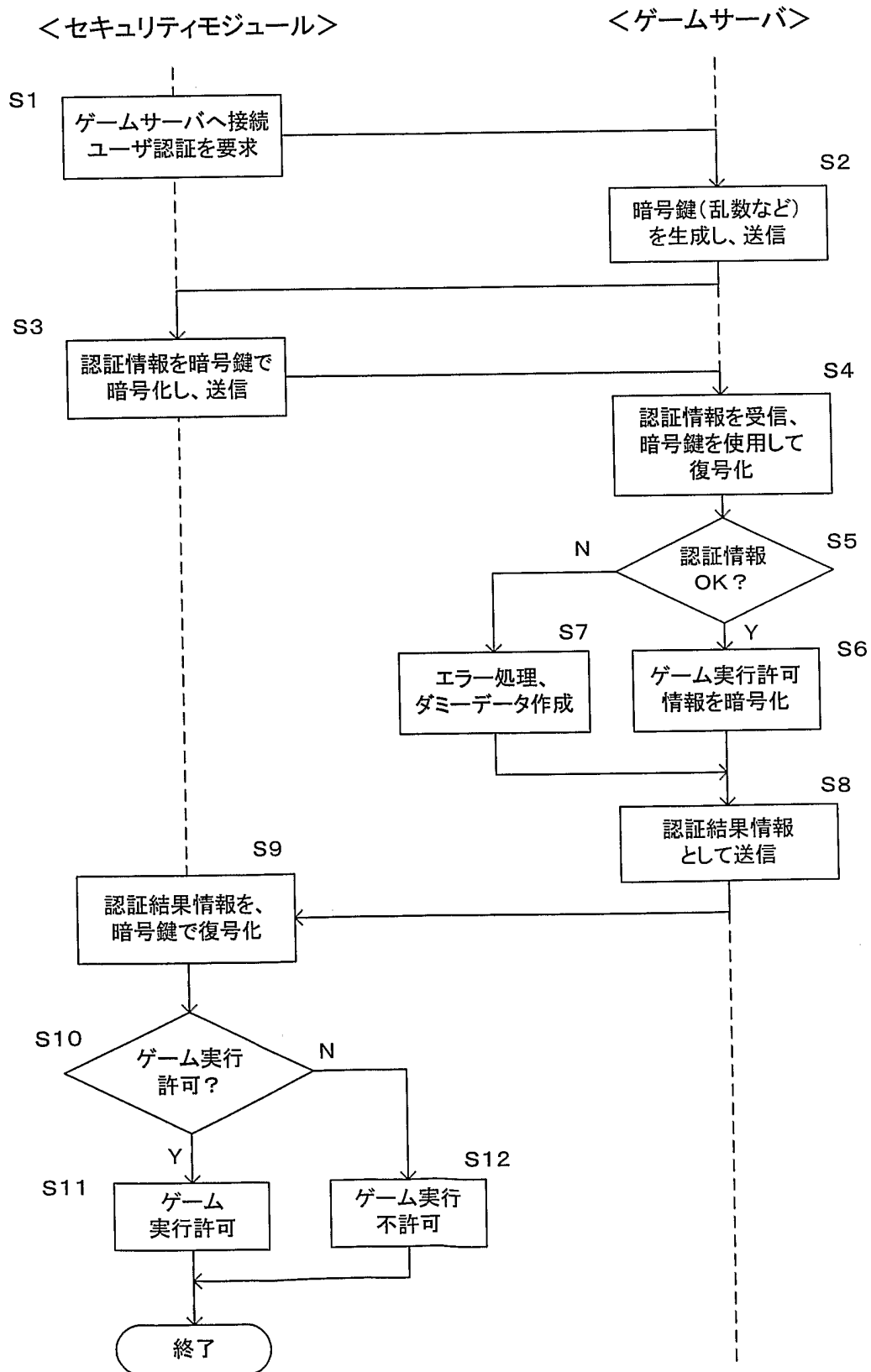
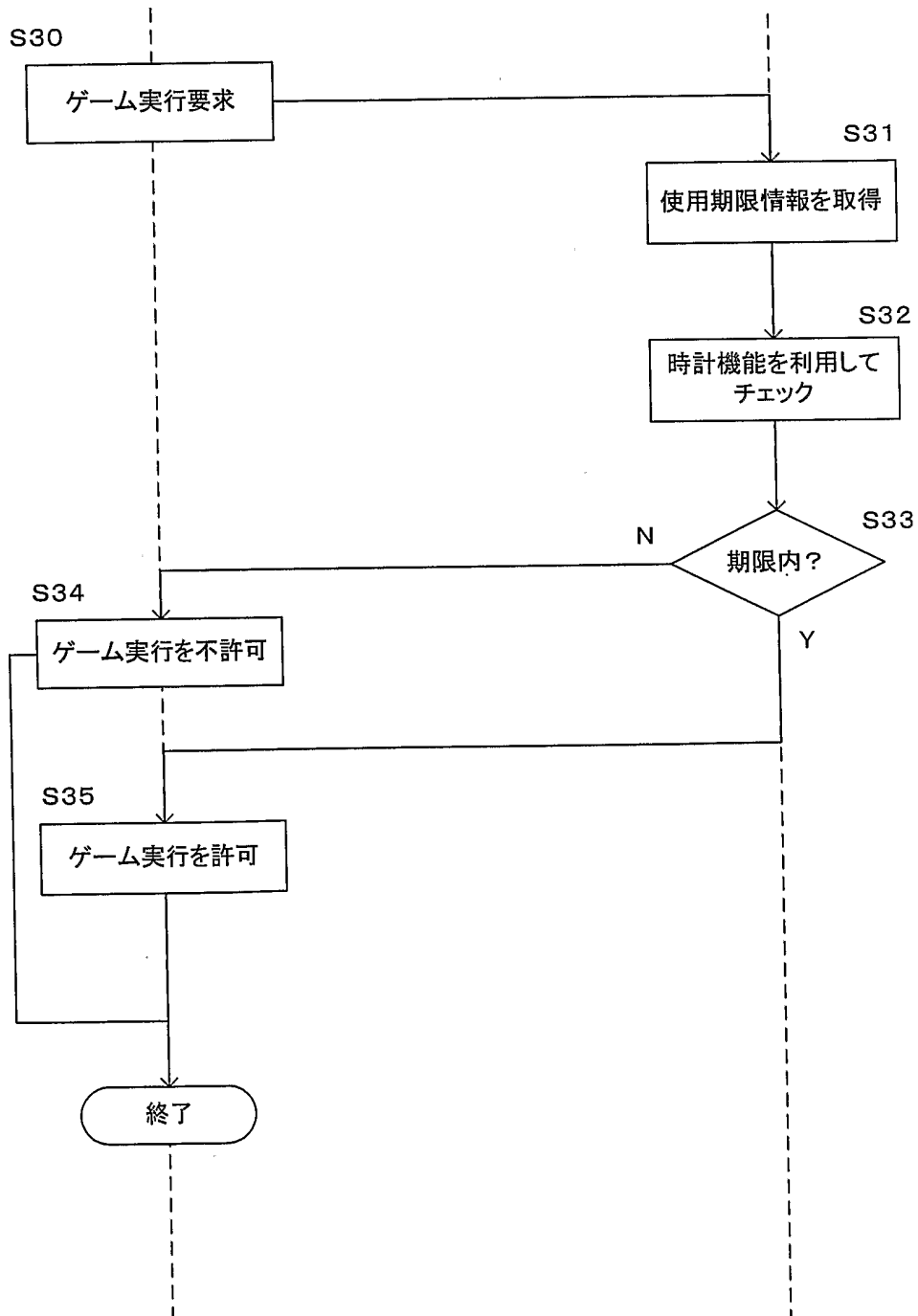


図5

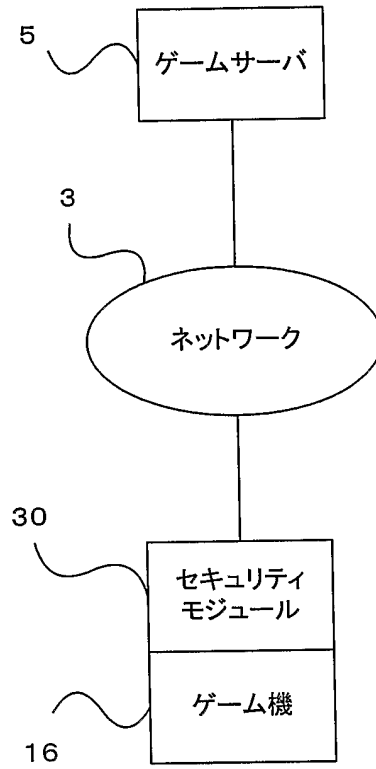
<ゲーム機>

<セキュリティモジュール>



6/6

図6



**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/JP03/11719

**A. CLASSIFICATION OF SUBJECT MATTER**  
Int.Cl<sup>7</sup> G06F15/00, H04L9/32, A63F13/12, A63F9/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F15/00, H04L9/32, A63F13/12, A63F9/00, G06F1/00,  
G06K19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2003  
Kokai Jitsuyo Shinan Koho 1971-2003 Toroku Jitsuyo Shinan Koho 1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 3-290733 A (Toshiba Corp.), 20 December, 1991 (20.12.91), Full text; all drawings (Family: none)	5 1-4
Y	JP 2001-159925 A (Suwacchi AG.), 12 June, 2001 (12.06.01), Claims; all drawings & CA 2319994 A1 & AU 6132500 A & CN 1293416 A	1-4
Y	JP 3-211932 A (Hitachi, Ltd. et al.), 17 September, 1991 (17.09.91), Claim 1 (Family: none)	1-4

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 18 December, 2003 (18.12.03)	Date of mailing of the international search report 13 January, 2004 (13.01.04)
---	---

Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/11719

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-66008 A (Sega Enterprises, Ltd.), 09 March, 1999 (09.03.99), Full text; all drawings (Family: none)	1-5
A	JP 2002-55961 A (Matsushita Electric Industrial Co., Ltd.), 20 February, 2002 (20.02.02), Full text; all drawings (Family: none)	1-5
A	JP 2002-251326 A (Hitachi, Ltd.), 06 September, 2002 (06.09.02), Full text; all drawings (Family: none)	1-5



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/11719

## Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1.  Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2.  Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3.  Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1 to 5 are divided into the following two groups:  
- Claims 1-4 relating to hardware for storing user authentication information, transmitting the authentication information to a server device, and allowing processing of the terminal device after authentication  
- Claim 5 relating to hardware having a clock for managing a use period of the terminal device

Since the technique for deciding to enable or disable a device processing according to the mounted hardware is a known technique, no technical relationship within the meaning of PCT Rule 13 between the different groups of inventions can be seen.

1.  As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2.  As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3.  As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4.  No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**  The additional search fees were accompanied by the applicant's protest.  
 No protest accompanied the payment of additional search fees.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F15/00, H04L9/32, A63F13/12, A63F9/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F15/00, H04L9/32, A63F13/12, A63F9/00  
G06F1/00, G06K19/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
日本国公開実用新案公報 1971-2003年  
日本国実用新案登録公報 1996-2003年  
日本国登録実用新案公報 1994-2003年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP 3-290733 A (株式会社東芝) 1991. 12. 20, 全文, 全図 (ファミリーなし)	5 1-4
Y	JP 2001-159925 A (スイッチ・アーゲー) 2001. 06. 12, 特許請求の範囲, 全図 & CA 2319994 A1 & AU 6132500 A & CN 1293416 A	1-4
Y	JP 3-211932 A (株式会社日立製作所他) 1991. 09. 17, 請求項1 (ファミリーなし)	1-4


C欄の続きにも文献が列挙されている。  パテントファミリーに関する別紙を参照。

\* 引用文献のカテゴリー  
 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」 口頭による開示、使用、展示等に言及する文献  
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献  
 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」 同一パテントファミリー文献

国際調査を完了した日 18. 12. 03

国際調査報告の発送日 13.01.04

国際調査機関の名称及びあて先  
 日本国特許庁 (ISA/JP)  
 郵便番号100-8915  
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)  
 宮司 卓佳  5B 9555  
 電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-66008 A (株式会社セガ・エンタープライゼス) 1999.03.09, 全文, 全図 (ファミリーなし)	1-5
A	JP 2002-55961 A (松下電器産業株式会社) 2002.02.20, 全文, 全図 (ファミリーなし)	1-5
A	JP 2002-251326 A (株式会社日立製作所) 2002.09.06, 全文, 全図 (ファミリーなし)	1-5

## 第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1.  請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2.  請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3.  請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるときこの国際調査機関は認めた。

請求の範囲第1項乃至第5項に係る発明は、以下の2群に区分される。

請求の範囲第1項乃至第4項

ユーザの認証情報を記憶し、該認証情報をサーバ装置に送信して認証を受けて端末装置の処理を許可するハードウェアに関するもの

請求の範囲第5項

時計部を持ち、端末装置の利用期限を管理するハードウェア

取り付けたハードウェアによって装置の処理の可否を決定する技術は周知であるから、上記2群の発明の間にはPCT規則13の意味における技術的な関連は見いだせない。

1.  出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2.  追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3.  出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4.  出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- 追加調査手数料の納付と共に出願人から異議申立てがあった。
- 追加調査手数料の納付と共に出願人から異議申立てがなかった。