(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4510366号
(P4510366)

(45)発行日　平成22年7月21日(2010.7.21)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330C
A63F 13/00	(2006.01)	A63F	13/00	A
A63F 13/12	(2006.01)	A63F	13/12	C

請求項の数 4　(全 17 頁)

(21)出願番号　特願2002-320424 (P2002-320424)
(22)出願日　平成14年11月1日 (2002.11.1)
(65)公開番号　特開2003-223416 (P2003-223416A)
(43)公開日　平成15年8月8日 (2003.8.8)
審査請求日　平成17年9月30日 (2005.9.30)
(31)優先権主張番号　10/011,253
(32)優先日　平成13年11月13日 (2001.11.13)
(33)優先権主張国　米国 (US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　リン　ティー．チェン
アメリカ合衆国　９８００６　ワシントン州　ベルビュー　１７４　プレイス　サウスイースト　５５３３

最終頁に続く

(54)【発明の名称】認証可能なゲームシステムを製造するためのアーキテクチャ

(57)【特許請求の範囲】

【請求項１】

オンラインサービスに参加する許可を与えるために、データセンタの認証サーバにおいて、ゲームコンソールを認証する方法であって、

前記ゲームコンソールの製造中に、製造コンピュータシステムが、

コンソールＩＤを各ゲームコンソールに割り当てることと、

対称鍵をランダムに生成することと、

前記対称鍵および前記コンソールＩＤを前記ゲームコンソールのメモリに記憶することと、

公開鍵ペアの公開鍵を使用して前記対称鍵を暗号化して暗号化された対称鍵を生成することと、

前記暗号化された対称鍵および前記コンソールＩＤをデータベースの中に記憶することとを含み、

前記データセンタにおける前記ゲームコンソールの認証中に、前記認証サーバが、

前記ゲームコンソールからの提供された対称鍵および前記コンソールＩＤを受け取ることと、

前記ゲームコンソールから受け取られた前記コンソールＩＤを使用して前記暗号化された対称鍵を含むレコードを前記データベースの中から探し出すことと、

予め記憶された公開鍵ペアの秘密鍵を使用して前記暗号化された対称鍵を暗号化解除して前記対称鍵を回復することと、

前記ゲームコンソールを認証するための基準として、前記暗号化された対称鍵から回復された前記対称鍵と前記ゲームコンソールから受け取られた前記提供された対称鍵との対応を評価することとを含むことを特徴とする方法。

【請求項２】

前記ゲームコンソールに記憶される対称鍵は前記製造コンピュータシステムによって公開鍵ペアの公開鍵を使用して暗号化されることを特徴とする、請求項１に記載の方法。

【請求項３】

ゲームコンソールのメモリの中にランダムに生成された対称鍵およびコンソールＩＤを書き込むように構成され、前記対称鍵を暗号化された形式でデータベースにさらに記憶する製造コンピュータシステムと、

前記ゲームコンソールからの提供された対称鍵および前記コンソールＩＤを受け取ることによって前記ゲームコンソールを認証するように構成され、前記コンソールＩＤを使用して暗号化された形式の前記対称鍵を探し出し、次に暗号化された対称鍵を回復するための予め記憶された秘密鍵を使用して前記対称鍵を暗号化解除し、前記ゲームコンソールを認証するための基準として、前記対称鍵を使用して前記ゲームコンソールから提供された対称鍵を評価する認証コンピュータシステムとを含むことを特徴とするシステム。

【請求項４】

ゲームコンソールのメモリの中にオリジナルの対称鍵およびコンソールＩＤを書き込むための書込み手段と、

公開鍵ペアの公開鍵を使用して前記オリジナルの対称鍵を暗号化して暗号化された対称鍵を生成するための暗号化手段と、を備える製造コンピュータシステムと、

前記暗号化された対称鍵を対応するコンソールＩＤとともに維持するための記憶手段と、

前記ゲームコンソールによってコンソールＩＤとともに提供された対称鍵と、前記提供されたコンソールＩＤに対応する前記暗号化された対称鍵から該暗号化された対称鍵を回復するための秘密鍵を使用して暗号化解除された前記オリジナルの対称鍵とを比較して、前記提供された対称鍵が前記オリジナルの対称鍵にマッチするかどうかを判定することによって前記ゲームコンソールを認証するための認証手段とを備える認証サーバとを含むことを特徴とするシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンソールベースのゲームシステムに関し、より詳細には、オンラインゲームなどのオンラインサービスへの参加のために認証することができるゲームコンソールを製造するためのシステムおよび方法に関する。

【０００２】

【従来の技術】

従来、専用コンソールを備えたゲームシステムは、限られた数のプレーヤ（例えば、４人）を受け容れる独立型マシンであった。ネットワーク（例えば、インターネット）を介して多数の遠隔のプレーヤとオンラインでゲームをすることができることにある程度、起因して、ＰＣベースのゲームが普及した。したがって、専用ゲームシステムの１つの動向は、オンラインゲームを円滑にするブロードバンド機能を提供することである。

【０００３】

専用コンソールのためにオンラインゲームアーキテクチャを作成することには、いくつかの固有の難しい問題がある。１つの問題は、様々なゲーム上の利点を得るため、オンラインゲーム中に不正行為を行おうと常に試みる何人かのハッカーが存在することである。この不正行為を阻止するため、ネットワークを介して伝送中のデータをハッカーによる観察および／または変更から保護するため、様々なセキュリティスキームが配備されている。しかし、そのようなスキームでは、遠隔のエンティティ（例えば、オンラインゲームサーバ、登録サーバ、その他のプレーヤシステム等）に対してゲームコンソールが自らを認証

することが必要とされる。ゲーム中のネットワークトラフィックの真正性を保証するため、認証中、有効な証明が使用される。登録中に、これらの証明を容易に獲得することが可能である場合、ハッカーは、その証明を容易に操作し、別のコンピュータを使用してビデオゲームコンソールからのすべてのネットワークパケットを偽造することができる。ゲームサーバの観点からは、そのゲームパケットは、必要とされる証明を提供することができたネットワークソースから来ているため、真性のものであるように見える。

【０００４】

【発明が解決しようとする課題】

したがって、オンラインゲームおよびその他のサービスを安全確実（secure）にするため、ハッカーが、不正行為を行う目的で、またはその他の不適切な使用の目的で有効な証明を容易に獲得するのを防止する必要が存在する。

【０００５】

【課題を解決するための手段】

コンソールベースのゲームシステムを製造するためのアーキテクチャは、製造中、既成の秘密をゲームコンソール上に配置し、後にその秘密を使用して、登録時中にそのゲームコンソールの真正性を保証することに関わる。

【０００６】

以下の２つの代表的な実施形態を説明する。対称鍵アーキテクチャ、および公開鍵アーキテクチャ。対称鍵アーキテクチャは、製造中、ランダムに生成された対称鍵をコンソールＩＤとともに、ゲームコンソールのプログラム式にアクセス可能な不揮発性メモリの中に書き込むことに関わる。対称鍵は、トランスポート中に公開鍵を使用して暗号化される。対応する秘密鍵、および暗号化された対称鍵は、認証エンティティにおいて安全確実に維持される。

【０００７】

登録中に、ゲームコンソールは、この鍵（または鍵の知識の証拠）とコンソールＩＤのペアを認証エンティティに発行（submit）する。このペアは、認証エンティティにおいて維持される対応する対称鍵を探し出すパスワード／名前ペアとして機能する。次に、秘密鍵を使用して対称鍵が暗号化解除（decrypt）される。ゲームコンソールによって発行された鍵は、そのコンソールが真性のものであるかどうかを判定する方策として、回復された対称鍵に照らして鑑定される。

【０００８】

公開鍵アーキテクチャは、製造中、各ゲームコンソールの中に秘密鍵およびデジタル証明書を書き込むことに関わる。この証明書は、秘密鍵に対応する公開鍵を含む。この証明書は、各製造現場における証明機関に関連する証明機関証明書、およびその証明機関証明書の導出元であるルート証明書を含む証明書連鎖の一部である。ゲームコンソールが登録のためにオンライン状態になるときはいつでも、そのコンソールが真性のものとして認証するのに、証明書連鎖検証プロセスが、そのゲームコンソール上に記憶された秘密鍵の知識（knowledge）の証拠とともに使用される。

【０００９】

【発明の実施の形態】

以下の説明は、オンライン接続性を有するコンソールベースのゲームシステム、およびインターネットなどのオープンなネットワークを介して遠隔の認証エンティティによってそのようなゲームシステムを認証できるような仕方で、そのようなゲームシステムを製造するための技法を対象とする。この技法は、ネットワークの反対側のエンティティが許可されたゲームシステムであることの保証をどのように認証エンティティが得ることができるかという問題に対処する。

【００１０】

この説明は、読者が、暗号化、暗号化解除（decryption）、認証、ハッシュ、デジタル署名、およびデジタル証明書などの基本的な暗号法の原理に精通していることを想定している。暗号法の基本的な概要に関しては、読者は、テキストを参照されたい（例えば、Bruc

e Schneierによる"Applied Cryptography: Protocols, Algorithms, and Source Code in C" (published by John Wiley & Sons, copyright 1994 (second edition 1996))という名称のテキスト参照）。このテキストは、参照により、本明細書に組み込まれる。

【００１１】

ゲームシステム

図１は、例としてのゲームシステム１００を示している。このゲームシステムは、ゲームコンソール１０２、およびコントローラ１０４（１）および１０４（２）で示した最高で４つのコントローラを含む。ゲームコンソール１０２は、内部ハードディスクドライブ、および光記憶ディスク１０８で示した様々な形態のポータブル記憶媒体をサポートするポータブルメディアドライブ１０６を備えている。適切なポータブル記憶媒体の例には、ＤＶＤ、ＣＤ－ＲＯＭ、ゲームディスク、ゲームカートリッジ、その他が含まれる。

【００１２】

ゲームコンソール１０２は、最高で４つのコントローラをサポートする４つのスロット１１０をその前面上に有するが、スロットの数および構成は、変更することができる。また、電源ボタン１１２およびイジェクトボタン１１４もゲームコンソール１０２の前面上に配置されている。電源ボタン１１２は、ゲームコンソールの電源の切り替えを行い、イジェクトボタン１１４は、ポータブルメディアドライブ１０６のトレイの開閉を交互に行って記憶ディスク１０８の挿入および引抜きを可能にする。

【００１３】

ゲームコンソール１０２は、Ａ／Ｖインターフェースケーブル１２０を介してテレビジョンまたはその他のディスプレイ（図示せず）に接続する。電源ケーブル１２２が、ゲームコンソールに給電を行う。ゲームコンソール１０２は、インターネットなどのネットワークに対するアクセスを円滑にするケーブルまたはモデムコネクタ１２４で示されるブロードバンド機能を備えるようにさらに構成することも可能である。

【００１４】

各コントローラ１０４は、有線インターフェースまたは無線インターフェースを介してゲームコンソール１０２に結合される。図示した実施形態では、コントローラは、ＵＳＢ（Universal Serial Bus）対応であり、シリアルケーブル１３０を介してコンソール１０２に接続される。コンソール１０２は、多種多様なユーザ対話機構を備えていることが可能である。図１に示す通り、各コントローラ１０４は、２つのサムスティック１３２（１）および１３２（２），Ｄパッド１３４、ボタン１３６、および２つのトリガ１３８を備えている。以上の機構は、単に代表的なものであり、図１に示したものに、その他の周知のゲーム機構を代用すること、または追加することが可能である。

【００１５】

メモリユニット（ＭＵ）１４０をコントローラ１０４に挿入して追加のポータブルストレージを提供することができる。ポータブルメモリユニットにより、ユーザは、他のコンソール上でゲームをするためにゲームパラメータを記憶して持ち運ぶことができるようになる。説明する実施形態では、各コントローラは、２つのメモリユニット１４０を収容するように構成されるが、他の実施形態では、２つより多い、または２つより少ないユニットを使用することができる。

【００１６】

ゲームシステム１００は、例えば、ゲーム、音楽、およびビデオを再生することができる。様々なストレージが提供されて、タイトルをハードディスクドライブ、またはドライブ１０６の中のポータブルメディア１０８から、またはオンラインソースから、またはメモリユニット１４０から再生することが可能である。ゲームシステム１００が再生することができるもののサンプルとして以下が含まれる。

【００１７】

１．ＣＤディスクおよびＤＶＤディスクから、ハードディスクドライブから、またはオンラインソースから再生されるゲームタイトル。

２．ポータブルメディアドライブ１０６の中のＣＤから、ハードディスクドライブ上のフ

ァイル（例えば、Windows（登録商標)Media Audio（ＷＭＡ）形式）から、またはオンラインストリームソースから再生されるデジタル音楽。
３．ポータブルメディアドライブ１０６の中のＤＶＤディスクから、ハードディスクドライブ上のファイル（例えば、Active Streaming形式）から、またはオンラインストリームソースから再生されるデジタルオーディオ／ビデオ。
【００１８】
図２は、ゲームシステム１００の機能上の構成要素をより詳細に示している。ゲームコンソール１０２は、中央処理装置（ＣＰＵ）２００と、フラッシュＲＯＭ（読取り専用メモリ）２０４、ＲＡＭ（ランダムアクセスメモリ）２０６、ハードディスクドライブ２０８、およびポータブルメディアドライブ１０６を含む様々なタイプのメモリに対するプロセッサアクセスを円滑にするメモリコントローラ２０２とを有する。ＣＰＵ２００は、一時的にデータを記憶し、したがって、メモリアクセスサイクルの回数を減少させ、これにより処理速度およびスループットを向上させるレベル１キャッシュ２１０およびレベル２キャッシュ２１２を備えている。
【００１９】
ＣＰＵ２００、メモリコントローラ２０２、および様々なメモリデバイスは、様々なバスアーキテクチャの任意のものを使用するシリアルバス、パラレルバス、メモリバス、周辺バス、およびプロセッサバスまたはローカルバスを含む１つ以上のバスを介して相互接続されている。例として、そのようなアーキテクチャには、インダストリスタンダードアーキテクチャ（Industry Standard Architecture）（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（Micro Channel Architecture）（ＭＣＡ）バス、エンハンストＩＳＡ（ＥＩＳＡ）バス、ビデオエレクトロニクススタンダーズアソシエーション（Video Electronics Standards Association）（ＶＥＳＡ）ローカルバス、およびペリフェラルコンポーネントインターコネクツ（Peripheral Component Interconnects）（ＰＣＩ）バスが含まれることが可能である。
【００２０】
１つの適切な実施形態として、ＣＰＵ２０、メモリコントローラ２０２、ＲＯＭ２０４、およびＲＡＭ２０６を共通モジュール２１４上に組み込むことができる。この実施形態では、ＲＯＭ２０４は、ＰＣＩ（ペリフェラルコンポーネントインターコネクツ）バスおよびＲＯＭバス（どちらも図示せず）を介してメモリコントローラ２０２に接続されるフラッシュＲＯＭとして構成される。ＲＡＭ２０６は、別個のバス（図示せず）を介してメモリコントローラ２０２によって独立に制御される複数のＤＤＲ　ＳＤＲＡＭ（Double Data Rate Synchronous Dynamic　ＲＡＭ）として構成される。ハードディスクドライブ２０８およびポータブルメディアドライブ１０６が、ＰＣＩバスおよびＡＴＡ（ＡＴ　Attachment）バス２１６を介してメモリコントローラに接続される。
【００２１】
３Ｄグラフィックス処理装置２２０およびビデオエンコーダ２２２が、高速かつ高解像度のグラフィックス処理のためのビデオ処理パイプラインを形成する。データは、グラフィックス処理装置２２０からビデオエンコーダ２２２にデジタルビデオバス（図示せず）を介して搬送される。オーディオ処理装置２２４およびオーディオＣＯＤＥＣ（エンコーダ／デコーダ）２２６が、高忠実度のステレオ処理を備えた対応するオーディオ処理パイプラインを形成する。オーディオデータは、通信リンク（図示せず）を介してオーディオ処理装置２２４とオーディオＣＯＤＥＣ２２６の間で搬送される。ビデオ処理パイプラインおよびオーディオ処理パイプラインは、テレビジョンまたはその他のディスプレイに伝送するためにデータをＡ／Ｖ（オーディオ／ビデオ）ポート２２８に出力する。図示する実施形態では、ビデオ処理構成要素およびオーディオ処理構成要素２２０－２２８が、モジュール２１４上に実装される。
【００２２】
また、モジュール２１４上には、ＵＳＢホストコントローラ２３０およびネットワークインターフェース２３２も実装される。ＵＳＢホストコントローラ２３０は、バス（例えば

、ＰＣＩバス）を介してＣＰＵ２００およびメモリコントローラ２０２に結合され、周辺コントローラ１０４（１）－１０４（４）のためのホストの役割をする。ネットワークインターフェース２３２は、ネットワーク（例えば、インターネット、ホームネットワーク等）に対するアクセスを提供し、イーサネット（登録商標）カード、モデム、Bluetoothモジュール、ケーブルモデム等を含む多種多様な様々な有線または無線のインターフェース構成要素であることが可能である。

【００２３】

ゲームコンソール１０２は、２つのゲームコントローラ１０４（１）－１０４（４）をそれぞれがサポートする２つのデュアルコントローラサポートサブアセンブリ２０４（１）および２０４（２）を有する。フロントパネルＩ／Ｏサブアセンブリ２４２は、電源ボタン１１２およびイジェクトボタン１１４の機能性をサポートし、またゲームコンソールの外面上に表出したあらゆるＬＥＤ（発光ダイオード）またはその他のインディケータをサポートする。サブアセンブリ２４０（１），２４０（２），および２４２は、１つ以上のケーブルアセンブリ２４４を介してモジュール２１４に結合される。

【００２４】

図では、８つのメモリユニット１４０（１）－１４０（８）が、４つのコントローラ１０４（１）－１０４（４）に、すなわち、各コントローラごとに２つのメモリユニットに接続可能である。各メモリユニット１４０は、ゲーム、ゲームパラメータ、およびその他のデータを記憶することができる追加のストレージを提供する。コントローラに挿入されたとき、メモリユニット１４０は、メモリコントローラ２０２によってアクセスされることが可能である。

【００２５】

システムパワーサプライモジュール２５０により、ゲームシステム１００の構成要素に給電が行われる。ファン２５２が、ゲームコンソール１０２内部の回路を冷却する。

【００２６】

コンソールユーザインターフェース（ＵＩ）アプリケーション２６０が、ハードディスクドライブ２０８上に記憶される。ゲームコンソールに電源が投入されたとき、コンソールアプリケーション２６０の様々な部分が、ＲＡＭ２０６および／またはキャッシュ２１０、２１２にロードされ、ＣＰＵ２００上で実行される。コンソールアプリケーション２６０は、ゲームコンソール上で利用可能な異なる媒体タイプにナビゲートする際、整合性のあるユーザ体験を提供するグラフィカルユーザインターフェースを提供する。

【００２７】

ゲームコンソール１０２は、暗号化、暗号化解除、認証、デジタル署名、ハッシュなどの一般的な暗号化機能を行う暗号化エンジンを実装する。暗号化エンジンは、ＣＰＵ２００の一部として実装し、またはＣＰＵ上で実行されるハードディスクドライブ２０８上に記憶されたソフトウェアとして実装して、暗号化機能をＣＰＵが実行するように構成することが可能である。

【００２８】

ゲームシステム１００は、システムを単にテレビジョンまたはその他のディスプレイに接続することによって独立型システムとして動作させることが可能である。この独立型モードでは、ゲームシステム１００により、１人以上のプレーヤが、ゲームを行うこと、映画を観ること、または音楽を聴くことができる。しかし、ネットワークインターフェース２３２を介して利用可能になるブロードバンド接続性が組み込まれると、ゲームシステム１００は、より広いネットワークゲームコミュニティの参加者としてさらに動作されることが可能である。次に、このネットワークゲーム環境を説明する。

【００２９】

ネットワークゲーム

図３は、ネットワーク３０２を介して複数のゲームシステム１００（１），．．．１００（ｇ）を相互接続する例としてのネットワークゲーム環境３００を示している。ネットワーク３０２は、多種多様なデータ通信網の任意のものを表す。ネットワーク３０２は、公

共部分（例えば、インターネット）およびプライベート部分（例えば、住宅のローカルエリアネットワーク（ＬＡＮ））、並びに公共部分とプライベート部分の組み合わせを含むことが可能である。ネットワーク３０２は、有線媒体と無線媒体の両方を含む多種多様な従来の通信媒体の任意の１つ以上を使用して実装することが可能である。公用のプロトコルと独自のプロトコルの両方を含め、多種多様な通信プロトコルの任意のものを使用して、ネットワーク３０２を介してデータを通信することができる。そのようなプロトコルの例には、ＴＣＰ／ＩＰ、ＩＰＸ／ＳＰＸ、ＮｅｔＢＥＵＩ等が含まれる。

【００３０】

ゲームシステム１００に加えて、１つ以上のデータセンタが、ネットワーク３０２を介してアクセス可能であり、参加者に対する様々なサービスを提供することが可能である。例としてのデータセンタ３０４が、個々のゲームシステム１００を登録する認証サーバ３０６と、オンラインゲームをホストすること、ダウンロード可能な音楽ファイルまたはビデオファイルを提供すること、ストリーミングオーディオ／ビデオファイルを提供することなどの様々なサービスを提供する１つ以上のオンラインサーバ３０８（１），．．．３０８（ｓ）を含むものとして図示されている。認証サーバ３０６は、製造中、個々のゲームシステム上に配置される製造秘密を記憶するデータベース３１０に対するアクセスを有する。これらの秘密は、ゲームシステムがオンラインゲームまたはその他のサービスに参加できるようにするのに先立ってゲームシステムを登録または認証するために使用される。

【００３１】

認証サーバ３０６、オンラインサーバ３０８、およびデータベース３１０が、データセンタ３０４を形成するように論理式にグループ化されるが、様々なコンピュータシステムが物理的に一緒に配置されるように、または同様の設備の一環であるようにしても、しなくてもよいことに留意されたい。さらに、図では、認証サーバ３０６は、オンラインサーバ３０８と別個であるが、認証機能性をサービスの一環として含めることも可能である。

【００３２】

ネットワークゲーム環境３００には、個々のプレーヤおよび／またはゲームシステム１００を互いに、またオンラインサービス３０４に対して認証する際にある役割をする鍵配信センタ３１２がさらに関与することが可能である。配信センタ３１２は、有効な参加者に鍵およびサービスチケットを配信し、次に、参加者が、その鍵およびチケットを使用して複数のプレーヤ間でゲームを構成すること、またはオンラインサービス３０８からサービスを購入することが可能である。配信センタ３１２は、データセンタ３０４に組み込むこと、または図示する通り、独立に存在することが可能である。

【００３３】

オンラインゲーム（またはその他のネットワークサービス）に参加するため、ゲームシステム１００は、まず、認証サーバ３０６によって認証されることを求める。オンラインサービスに参加する許可を与えるのに、認証サーバ３０６は、各ゲームシステムが真性であり、不適切なコンピュータ装置でないことを信頼する必要がある。真性のゲームシステム１００は、秘密がデータベース３１０の中に記憶されて製造されている。認証サーバ３０６は、これらの秘密を使用して、ゲームシステム１００が真性であるかどうかを識別する。次節で、インターネットなどのオープンネットワークを介してオンラインゲームのために認証されることが可能なゲームシステムを製造するための技法を説明する。

【００３４】

認証されると、ゲームシステムは、オンラインゲームまたはその他のサービスに参加すること、または鍵配信センタを使用して個々のユーザの認証に取りかかることができる。マルチユーザ認証アーキテクチャが、より詳細に説明されている（例えば、２００１年3月９日出願の「Multiple User Authentication for Online Console-Based Gaming」という名称の米国特許出願、シリアル番号０９／８０２７９５参照）。この出願は、Microsoft（登録商標） Corporationに譲渡され、参照により、本明細書に組み込まれる。

【００３５】

認証可能なゲームシステムを製造すること

コンソール認証問題に対処するゲームシステムを製造するためのアーキテクチャを提供する。簡単に述べると、問題は、どのように認証エンティティが、ネットワークの反対側のエンティティが真性のゲームコンソールであるという確証を得ることができるかということである。本アーキテクチャは、一般に、製造中にゲームコンソール上に認証可能なデータである秘密を記憶し、対応する検証データを認証エンティティにおいて維持することに関わる。登録中に、認証エンティティは、その検証データを使用して、ゲームコンソールによって発行された認証可能なデータを検証してゲームコンソールの真正性を判定する。以下の２つの代表的なアーキテクチャを説明する。（１）対称鍵アーキテクチャ、および（２）公開鍵アーキテクチャ。

【００３６】

対称鍵アーキテクチャ

対称キーアーキテクチャは、製造中、ランダムに生成された対称鍵をコンソールＩＤとともにゲームコンソール上に書き込むことに関わる。後に、この鍵／ＩＤペアは、登録中に、ゲームコンソールが真性であることを認証サーバに証明するパスワード／名前ペアとして機能する。製造プロセスを示す図４、および登録プロセスを示す図５を参照して本アーキテクチャを説明する。

【００３７】

図４は、製造中、対称鍵およびコンソールＩＤがゲームコンソール上に配置されるれ例としての製造プロセス４００を示している。説明のため、製造業者は、１つ以上の製造コンピュータシステム４５０および製造データベース４５２をそれぞれが含む１つ以上の製造設備を運用するものとする。製造データベースは、ときとして、「系統データベース」と呼ばれる。製造コンピュータシステム４５０は、ゲームコンソールに配置されるソフトウェア／ファームウェアをプログラミングする、構成する、または別の仕方でイネーブル状態にするのに使用される。

【００３８】

工程４０２において、固有識別子Ｎｉが、それぞれの製造されたコンソール１０２（ｉ）に割り当てられる。コンソールＩＤは、例えば、製造されたコンソールの連番または通し番号であることが可能である。工程４０４において、対称鍵Ｋｉが、コンソール１０２（ｉ）のためにランダムに生成される。工程４０６において、対称鍵Ｋｉおよびコンソール識別子Ｎｉが、コンソール１０２（ｉ）のプログラム式にアクセス可能な不揮発性メモリの中に記憶される。記憶の場所は、好ましくは、ゲームコンソール所有者によるアクセスから安全（secure）であり、かつ／または秘密であるが、それ以外では、許可されたゲームコンソールによってプログラム式にアクセス可能である。可能な場所には、ＥＥＰＲＯＭ、ハードドライブ、またはフラッシュＲＯＭが含まれるが、以上には限定されない。また、Ｋｉ／Ｎｉペアを暗号式に保護して、ゲームコンソール所有者によるアクセスをさらに防止することができる。

【００３９】

Ｋｉ／Ｎｉペアは、登録プロセス中に使用されてゲームコンソールの真正性を証明する。したがって、Ｋｉ／Ｎｉペアは、ゲームコンソールを登録することを担うデータセンタ３０４への転送のため、製造中に収集される。ただし、鍵／ＩＤペアの転送および記憶は、発見される可能性のリスクを導入する。記憶および転送に関して対称鍵のセキュリティを確保するため、対称鍵は、対称鍵Ｋｉが生成された直後に転送公開鍵Ｋｔ＿ｐｕｂを使用して暗号化され、ゲームコンソールの中に記憶される（工程４０８）。暗号化解除を行って対称鍵Ｋｉにアクセスするのに使用される対応する転送秘密鍵Ｋｔ＿ｐｒｖは、データセンタ３０４において安全確実に維持され、ゲームコンソールの登録中に使用されるときだけにアクセスされる。

【００４０】

工程４０４－４０８の１つ以上が、製造コンピュータシステム４５０によって行われる、あるいは、ゲームコンソール自体によって行われるのが可能であることに留意されたい。鍵Ｋｉがどこで生成され、暗号化されるかに関わらず、目標は、この鍵が生の状態で存在

する時間を可能な限り短くすることである。この時間を最小限に抑えることにより、セキュリティがさらに高まる。

【００４１】

対称鍵Ｋｉは、公開鍵暗号以外の暗号法上の暗号を使用して暗号化できることにさらに留意されたい。例えば、対称鍵暗号を使用して、製造業者およびデータセンタにおいて安全確実に維持される対称鍵Ｋｉを暗号化することができる。

【００４２】

工程４１０において、暗号化された対称鍵（Ｅ（Ｋｔ＿ｐｕｂ，Ｋｉ）で示す）が、コンソール識別子Ｎｉとともに製造業者データベース４５２の中に記憶される。工程４１２において、すべての製造されたコンソールに関するコンソール識別子Ｎｉおよび暗号化された対称鍵（Ｅ（Ｋｔ＿ｐｕｂ，Ｋｉ）が、製造業者データベース４５２からデータセンタ３０４に個々に、または一括で転送される。この情報は、ネットワークを介する電子式伝送、ポータブル記憶媒体上の安全確実な輸送、またはその他の手段による任意のいくつかの異なる技法に従って転送することができる。

【００４３】

この時点で、ゲームコンソールは、製造が終了し、流通および販売のために梱包される。ゲームコンソールが購入された後、所有者が、ゲームをすること、またはオーディオ／ビデオファイルをダウンロードすることなどのオンラインサービスに参加するのを望むことが可能である。ゲームコンソールは、オンラインサービスに最初に遭遇したとき、登録プロセスを行って自らの真正性をそのオンラインサービスに対して証明する。説明のため、ゲームコンソールが、データセンタ３０４の認証サーバ３０６に登録して、１つ以上のオンラインサーバ３０８によってホストされているオンラインゲームイベントに参加できるようになるものと想定する。

【００４４】

図５は、データセンタ３０４における認証サーバ３０６がゲームコンソール１０２（ｉ）を認証する例としての登録プロセス５００を示している。工程５０２において、コンソール１０２（ｉ）が、認証プロトコルの一環として、対称鍵（または鍵の知識の証拠）とコンソールＩＤのペア（例えば、Ｋｉ，Ｎｉ）をデータセンタ３０４における認証サーバ３０６に発行する。対称鍵Ｋｉは、通常、認証プロトコル中に何らかの形で保護され、一方、コンソール識別子Ｎｉは、保護される必要がない。この工程中、Ｋｅｒｂｅｒｏｓ、Ｄｉｇｅｓｔ、およびＨＴＴＰ　Ｂａｓｉｃを含む多くの異なる認証プロトコルを使用することができる。ネットワークを介する通信はすべて、オプションとして、安全なチャネル（例えば、ＳＳＬチャネル）内でセキュリティ確保することができる。

【００４５】

工程５０４において、認証サーバ３０６が、コンソール識別子Ｎｉを使用して製造業者の秘密データベース３１０の中で関連する対称鍵をルックアップする。このルックアップの結果、コンソール１０２（ｉ）に関するデータレコード５２０がもたらされる。データレコード５２０は、図４の製造プロセス４００において製造業者によって元々、作成され、そこから転送された暗号化された対称鍵（Ｅ（Ｋｔ＿ｐｕｂ，Ｋｉ）を含む。工程５０６において、認証サーバ３０６が、認証サーバ３０６において記憶されている転送秘密鍵Ｋｔ＿ｐｒｖを使用してその対称鍵を暗号化解除して、対称鍵Ｋｉを回復する。

【００４６】

工程５０８において、認証サーバ３０６が、一つには、発行された鍵Ｋｉ（または鍵の知識（knowledge）の証拠）を製造業者の秘密データベース３１０の中のレコード５２０から回復された製造業者によって割り当てられた対称鍵Ｋｉと比較することにより、ゲームコンソール１０２（ｉ）によって発行された証明を検証する。認証サーバは、認証が成功したか、または失敗したかに基づいてゲームコンソールの受入れ、または拒否を行い、この成功、または失敗は、少なくとも部分的には２つの鍵がマッチしたかどうかに基づく。

【００４７】

この時点で、認証の結果を使用してオンラインサービスへの参加を直接に許可／拒否する

ことが可能である。このケースでは、ゲームコンソールがオンラインサービスに参加する目的で認証を要求するたびに毎回、対称鍵が使用される。あるいは、認証の結果を使用して、新しい一組の証明が生成され、オンラインサービス認証中に後の使用のためにゲームコンソールに転送される新規証明プロセスのブートストラップを行うことが可能である。この第２のケースでは、Ｋｉ／Ｎｉペアは、ゲームコンソールの登録中に、認証のために一回だけ使用されて、登録プロセスは、それ以降、使用することができる新しい一組の証明をコンソールに戻す。

【００４８】

対称鍵アーキテクチャの利点は、製造業者において秘密が全く維持されないことである。秘密の転送秘密鍵は、データセンタにおいて保持される。したがって、不正を行う人が秘密を盗む機会が大幅に減少する。

【００４９】

公開鍵アーキテクチャ

公開鍵アーキテクチャは、製造中、各ゲームコンソールに秘密鍵およびデジタル証明書を書き込むことに関わる。証明書は、秘密鍵にマッチする公開鍵を含む。各製造現場に配置された証明機関によってその証明書に署名が行われる。証明書連鎖を辿って最終的にはルート証明書にまで至る別の証明書によって各証明機関証明書にさらに署名が行われる。ゲームコンソールがオンライン状態になって自らを登録するときにはいつでも、そのコンソールを真性のものとして認証するのに、証明書連鎖検証プロセス、並びに秘密鍵の知識（knowledge）の証拠が使用される。製造前プロセスを示す図６、および製造プロセスを示す図７、および登録プロセスを示す図８を参照して公開鍵アーキテクチャを説明する。

【００５０】

図６は、公開鍵ペアおよび連鎖の証明書が生成される例としての製造前プロセス６００を示している。プロセス６００は、ゲームコンソール１０２の製造前の任意の時点で行われることが可能である。このプロセスは、製造設備において、または別の場所で行われることが可能である。工程６０２において、ルート公開鍵Ｋｒｏｏｔ＿ｐｕｂおよびルート秘密鍵Ｋｒｏｏｔ＿ｐｒｖから成るルート公開鍵ペアが生成される。このルート鍵ペアは、信頼され、安全確実（secure）に記憶される。

【００５１】

工程６０４において、ルート鍵ペアを使用してルート証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｒｏｏｔ＿ｐｕｂ）を生成する。「ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｒｏｏｔ＿ｐｕｂ）」という表記は、ルート公開鍵の真正性を、対応するルート秘密鍵を知るいずれの者に対しても保証するルート公開鍵Ｋｒｏｏｔ＿ｐｕｂと目的ステートメントの合成にデジタル署名を行うのに使用されるルート秘密鍵Ｋｒｏｏｔ＿ｐｒｖを意味する。したがって、ルート公開鍵Ｋｒｏｏｔ＿ｐｕｂにアクセスを有するいずれの者も、証明書の真正性を検証できるはずである。一例のタイプの証明書が、Ｘ．５０９形式の証明書である。ただし、別の秘密鍵で署名された公開鍵を担うその他のタイプのデータ構造も、証明書とみなすことができる。

【００５２】

工程６０６において、第２の公開鍵ペアが、製造現場における証明機関（ＣＡ）による使用のために生成される。この第２の鍵ペアは、証明機関鍵ペア（またはＣＡ鍵ペア）と呼ばれ、ＣＡ公開鍵Ｋｃａ＿ｐｕｂとＣＡ秘密鍵Ｋｃａ＿ｐｒｖから成る。各製造現場において複数の証明機関が存在する場合、各証明機関ごとに異なるＣＡ鍵ペアが生成される。したがって、各製造現場が１つ以上のＣＡ鍵ペアに関連付けられる。

【００５３】

工程６０８において、証明機関に関するＣＡ証明書が生成され、ルート秘密鍵Ｋｒｏｏｔ＿ｐｒｖで署名が行われる。ＣＡ証明書は、ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）として示され、これは、ＣＡ秘密鍵を知る任意のエンティティに対してＣＡ公開鍵の真正性を保証するＣＡ公開鍵Ｋｃａ＿ｐｕｂと目的ステートメントの合成にデジタル署名を行うのに、ルート秘密鍵Ｋｒｏｏｔ＿ｐｒｖが使用されることを意味する。

【００５４】
工程６１０において、ＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）およびＣＡ秘密鍵が、製造現場における証明機関６５０において記憶される。ＣＡ証明書およびＣＡ秘密鍵Ｋｃａ＿ｐｒｖは、漏洩を防止するように安全確実（secure）な仕方で維持される。工程６１２において、ルート公開鍵Ｋｒｏｏｔ＿ｐｕｂおよび／またはルート証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｒｏｏｔ＿ｐｕｂ）が、データセンタ３０４に転送され（遠隔で生成される場合）、安全確実な仕方で記憶される。
【００５５】
図７は、製造中、秘密鍵および１つ以上の証明書がゲームコンソール上に配置される例としての製造プロセス７００を示している。製造のため、製造業者は、ＣＡ公開鍵ペア（Ｋｃａ＿ｐｕｂ，Ｋｃａ＿ｐｒｖ）およびＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）を維持する。
【００５６】
工程７０２において、それぞれの製造されたコンソール１０２（ｉ）に関するゲームコンソール公開鍵ペアが生成される。コンソール公開鍵ペアは、コンソール公開鍵Ｋｉ＿ｐｕｂとコンソール秘密鍵Ｋｉ＿ｐｒｖから成る。工程７０４において、コンソール証明書ＣＥＲＴ（Ｋｃａ＿ｐｒｖ，Ｋｉ＿ｐｕｂ）が生成され、工場における証明機関のＣＡ秘密鍵Ｋｃａ＿ｐｒｖで署名が行われる。このコンソール証明書は、公開鍵Ｋｉ＿ｐｕｂを含み、コンソール秘密鍵Ｋｉ＿ｐｒｖを知るどのエンティティに対してもそのコンソールの真正性を保証する。
【００５７】
工程７０６において、製造業者が、コンソール秘密鍵Ｋｉ＿ｐｒｖ、コンソール証明書ＣＥＲＴ（Ｋｃａ＿ｐｒｖ，Ｋｉ＿ｐｕｂ），およびＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）をゲームコンソールの中に記録する。記憶の場所は、鍵および証明書が、許可されたゲームコンソールによってプログラム式にアクセス可能であるが、ゲームコンソール所有者によるアクセスからは安全であるようにする。可能な場所には、ＥＥＰＲＯＭ、ハードドライブ、またはフラッシュ可能なＲＯＭが含まれるが、それらには限定されない。ＣＡ秘密鍵Ｋｃａ＿ｐｒｖは、製造現場においてセキュリティ確保されるが、公開鍵および証明書を含むその他すべての情報は、セキュリティ対策なしに自由に配布することができる。
【００５８】
図８は、ゲームコンソールが、データセンタ３０４における認証サーバ３０６によって認証される例としての登録プロセス８００を示している。多数の異なる公開鍵認証プロトコルを使用して登録プロセスを実施することができる。登録時に、認証サーバ３０６が、ルート証明書に（また、したがって、ルート公開鍵に）アクセスする。
【００５９】
工程８０２において、適切なプロトコルの一環として、コンソール１０２（ｉ）が、データセンタ３０４における認証サーバ３０６にコンソール証明書ＣＥＲＴ（Ｋｃａ＿ｐｒｖ，Ｋｉ＿ｐｕｂ）を送信する。コンソールは、オプションとして、認証サーバがＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）を既に所有しているのではない場合、ＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）を送信することができる。また、コンソールは、自らがコンソール秘密鍵Ｋｉ＿ｐｒｖを知っているという何らかの証拠を発行する。この証拠は、多くの仕方で獲得することができる。そのような証拠を提供するための１つの手法は、コンソール秘密鍵Ｋｉ＿ｐｒｖを使用して何らかのデータを暗号化することである。このデータは、例えば、現在時刻、乱数、メッセージ等であることが可能である。以下の説明では、コンソールは、現在時刻をコンソール秘密鍵を使用して暗号化する、つまりＥ（Ｋｉ＿ｐｒｖ，ＣｕｒｒｅｎｔＴｉｍｅ）であると想定する。現在時刻を使用することは、リプレイ攻撃を阻むのに役立つ可能性がある。
【００６０】
次に、認証サーバ３０６が、証明書連鎖認証プロセスを行ってコンソール証明書まで証明

書連鎖をトラバース（traverse）する。より具体的には、工程８０４で、認証サーバ３０６が、公開鍵Ｋｒｏｏｔ＿ｐｕｂを使用してＣＡ証明書の署名を検証することによってＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）を認証する。ルート公開鍵は、認証サーバにおいて記憶する、またはルート証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｒｏｏｔ＿ｐｕｂ）から抽出することが可能である。工程８０６において、認証サーバ３０６が、ＣＡ証明書からＣＡ公開鍵Ｋｃａ＿ｐｕｂを獲得し、それを使用してコンソール証明書ＣＥＲＴ（Ｋｃａ＿ｐｒｖ，Ｋｉ＿ｐｕｂ）の署名を検証して、これにより、そのコンソール証明書を認証する。

【００６１】

工程８０８において、認証サーバ３０６は、コンソール証明書から取り出したコンソール公開鍵Ｋｉ＿ｐｕｂを使用してコンソール秘密鍵Ｋｉ＿ｐｒｖの知識の証拠を評価する。認証サーバ３０６が、コンソールが正しいコンソール秘密鍵の知識を有することを発行された証拠を介して検証できる場合、そのゲームコンソール１０２（ｉ）は、真性のものとして信頼される。現在時刻を使用する本例では、認証サーバは、コンソール公開鍵を使用して、コンソールによって発行された暗号化された現在時刻を暗号化解除する。回復された現在時刻は、許容可能な時間スキューの範囲内にあると検証される。ゲームサーバは、認証が成功したか、または失敗したかに基づいてゲームコンソールの受入れ、または拒否を行い、この成功または失敗は、回復された時間が時間スキューの範囲内にあるかどうかに少なくとも部分的に基づく。

【００６２】

この時点で、認証の結果を使用して、オンラインサービスへの参加を直接に許可／拒否することが可能である。このケースでは、ゲームコンソールが、オンラインサービスに参加する目的で認証を要求するたびに毎回、同じ登録プロセスが使用される。あるいは、認証の結果を使用して、新しい一組の証明が生成され、オンラインサービス認証中に後の使用のためにゲームコンソールに転送される新規証明プロセスのブートストラップを行うことが可能である。この第２のケースでは、コンソール秘密鍵Ｋｉ＿ｐｒｖ、コンソール証明書ＣＥＲＴ（Ｋｃａ＿ｐｒｖ，Ｋｉ＿ｐｕｂ），およびＣＡ証明書ＣＥＲＴ（Ｋｒｏｏｔ＿ｐｒｖ，Ｋｃａ＿ｐｕｂ）の証明が、登録中に、認証のために一回だけ使用され、登録プロセスは、それ以降、使用することができる新しい一組の証明をコンソールに戻す。

【００６３】

本明細書で説明する公開鍵アーキテクチャは、ルート証明書からコンソール証明書に至る２つのレベルの証明書連鎖を使用していることに留意されたい。より多い、またはより少ないレベルの証明書連鎖を使用して本アーキテクチャを実施することも可能である。

【００６４】

公開鍵アーキテクチャの利点は、コンソール製造現場とデータセンタにおける認証サーバの間で鍵の転送が全く行われないことである。ただし、公開鍵アーキテクチャでは、製造業者において秘密が維持される。

【００６５】

結論

本発明は、構造上の特徴および／または方法上の処置に固有の言い回しで説明してきたが、頭記の特許請求の範囲で定義する本発明は、必ずしも説明した特定の特徴および特定の処置に限定されないことを理解されたい。むしろ、特定の特徴および特定の処置は、請求する本発明を実施する例としての形態として開示している。

【図面の簡単な説明】

【図１】ゲームコンソールおよび１つ以上のコントローラを有するゲームシステムを示す図である。

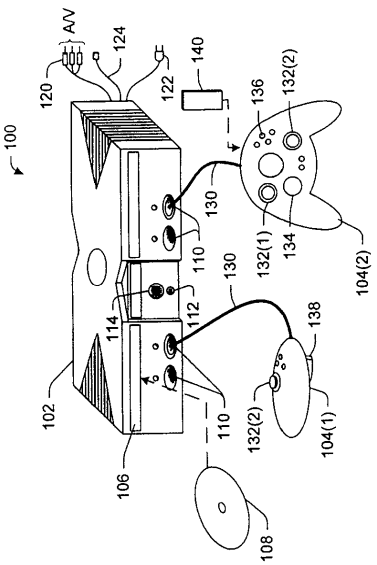
【図２】ゲームシステムを示すブロック図である。

【図３】図１のゲームシステムが、ネットワークを介して他のコンソール、サービス、およびチケット発行エンティティに接続されているネットワークゲームシステムを示す図である。

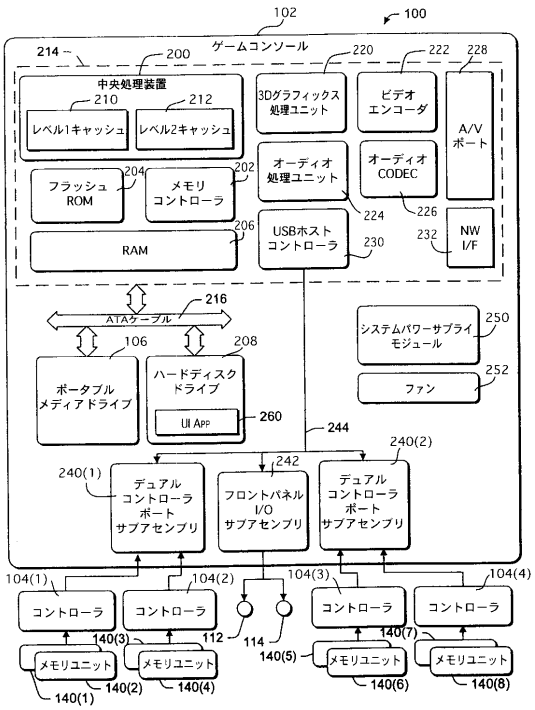
【図４】製造中に、対称鍵およびコンソールＩＤがゲームコンソール上に配置される製造プロセスを示す図である。
【図５】認証サーバが、対称鍵およびコンソールＩＤを使用してゲームコンソールを認証する登録プロセスを示す図である。
【図６】公開鍵ペアおよび連鎖証明書が最初に生成される製造前プロセスを示す図である。
【図７】製造中に、秘密鍵および１つ以上の証明書がゲームコンソール上に配置される製造プロセスを示す図である。
【図８】認証サーバが、秘密鍵および証明書検証プロセスを使用してゲームコンソールを認証する登録プロセスを示す図である。
【符号の説明】
１００（１），１００（ｇ）　ゲームシステム
１０２　ゲームコンソール
１０４（１），１０４（２），１０４（３），１０４（４）　コントローラ
１０６　ポータブルメディアドライブ
１０８　ポータブル記憶媒体
１１０　スロット
１１２　電源ボタン
１１４　イジェクトボタン
１２０　Ａ／Ｖインターフェースケーブル
１２２　電源ケーブル
１２４　モデムコネクタ
１３０　シリアルケーブル
１３２（１），１３２（２）　サムスティック
１３４　Ｄパッド
１３６　ボタン
１３８　トリガ
１４０（１），１４０（２），１４０（３），１４０（４），１４０（５），１４０（６），１４０（７），１４０（８）　メモリユニット
２００　中央処理装置
２０２　メモリコントローラ
２０４　フラッシュＲＯＭ
２０６　ＲＡＭ
２０８　ハードディスクドライブ
２１０，２１２　キャッシュ
２１６　ＡＴＡケーブル
２２０　３Ｄグラフィックス処理ユニット
２２２　ビデオエンコーダ
２２４　オーディオ処理ユニット
２２６　オーディオＣＯＤＥＣ
２２８　Ａ／Ｖポート
２３０　ＵＳＢホストコントローラ
２４０（１），２４０（２），２４２　サブアセンブリ
２５０　システムパワーサプライモジュール
２５２　ファン
３００　ネットワーク環境
３０２　ネットワーク
３０４　データセンタ
３０６　認証サーバ
３０８（１），３０８（ｓ）　オンラインサーバ

３１０　データベース
３１２　鍵配信センタ

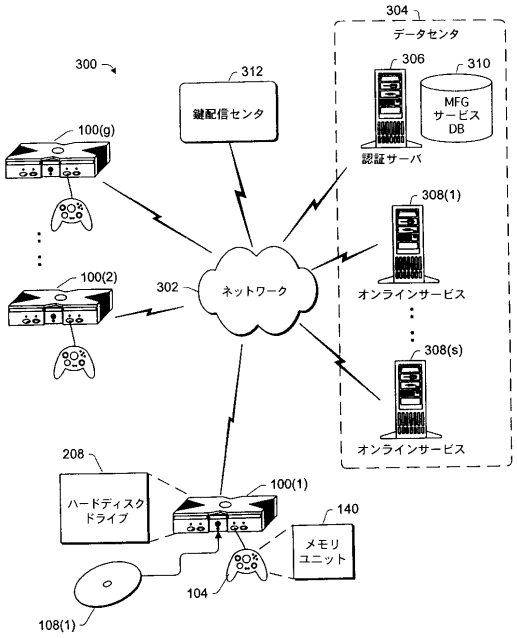
【図１】



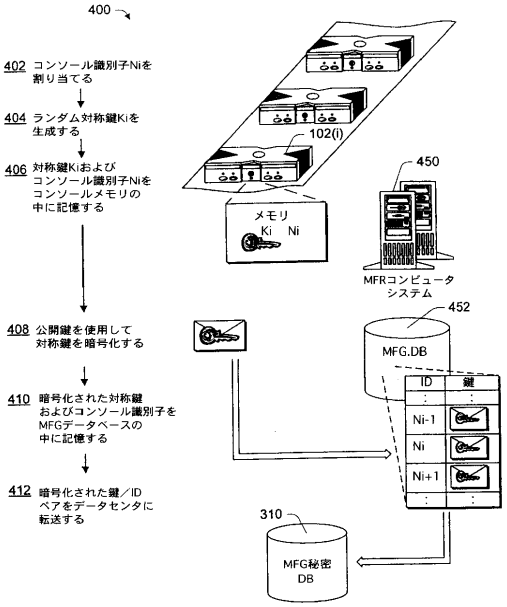
【図２】



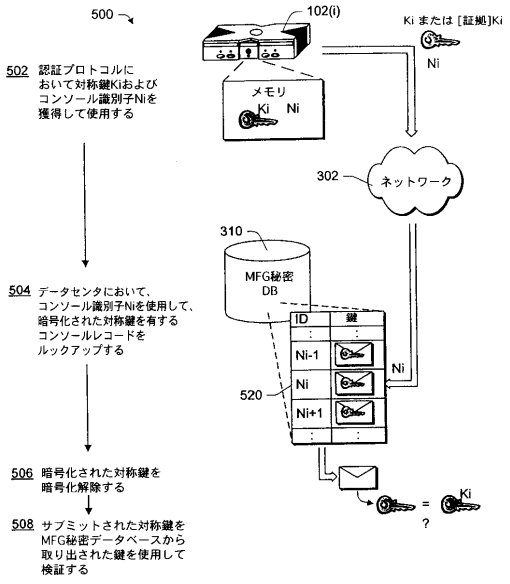
【図３】


304
データセンタ
306
310
MFG
サービス
DB
認証サーバ
300
312
鍵配信センタ
100(g)
308(1)
オンラインサービス
100(2)
302
ネットワーク
308(s)
オンラインサービス
208
ハードディスク
ドライブ
100(1)
140
メモリ
ユニット
104
108(1)

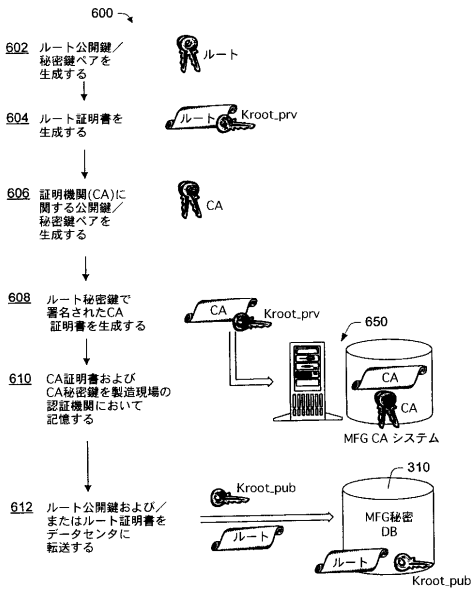
【図４】


400
402 コンソール識別子Niを
割り当てる
404 ランダム対称鍵Kiを
生成する
406 対称鍵Kiおよび
コンソール識別子Niを
コンソールメモリの
中に記憶する
408 公開鍵を使用して
対称鍵を暗号化する
410 暗号化された対称鍵
およびコンソール識別子を
MFGデータベースの
中に記憶する
412 暗号化された鍵／ID
ペアをデータセンタに
転送する
102(i)
メモリ
Ki Ni
450
MFRコンピュータ
システム
452
MFG.DB
ID
鍵
Ni-1
Ni
Ni+1
310
MFG秘密
DB

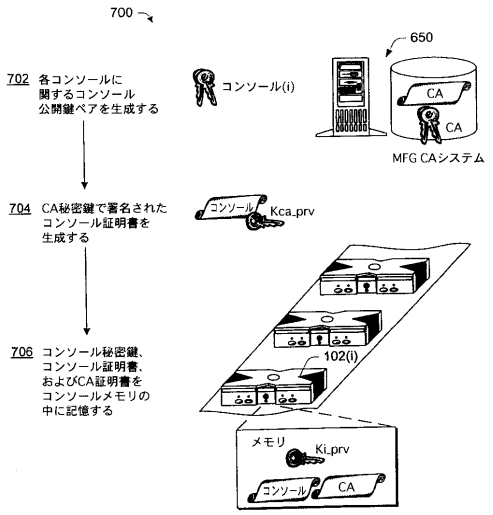
【図５】


500
502 認証プロトコルに
おいて対称鍵Kiおよび
コンソール識別子Niを
獲得して使用する
504 データセンタにおいて、
コンソール識別子Niを使用して、
暗号化された対称鍵を有する
コンソールレコードを
ルックアップする
506 暗号化された対称鍵を
暗号化解除する
508 サブミットされた対称鍵を
MFG秘密データベースから
取り出された鍵を使用して
検証する
102(i)
Ki または [証拠]Ki
Ni
メモリ
Ki Ni
302
ネットワーク
310
MFG秘密
DB
ID
鍵
Ni-1
Ni
Ni+1
520
Ni
Ki
=
?

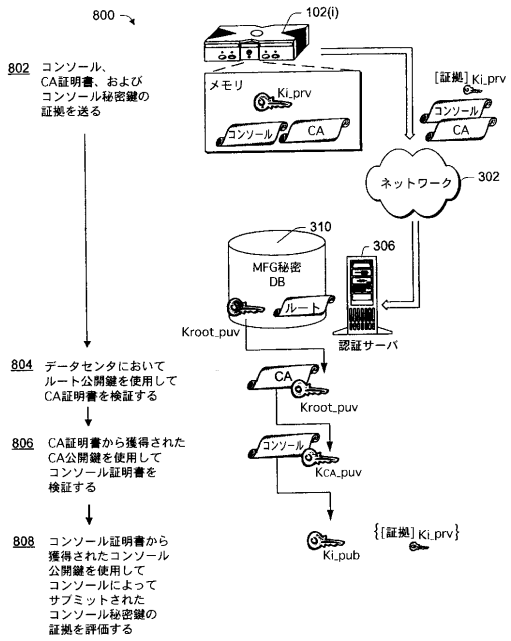
【図６】


600
602 ルート公開鍵／
秘密鍵ペアを
生成する
604 ルート証明書を
生成する
606 証明機関(CA)に
関する公開鍵／
秘密鍵ペアを
生成する
608 ルート秘密鍵で
署名されたCA
証明書を生成する
610 CA証明書および
CA秘密鍵を製造現場の
認証機関において
記憶する
612 ルート公開鍵および／
またはルート証明書を
データセンタに
転送する
ルート
ルート
Kroot_prv
CA
CA
Kroot_prv
650
CA
CA
MFG CA システム
Kroot_pub
ルート
310
MFG秘密
DB
ルート
Kroot_pub

【図７】


700
702 各コンソールに関するコンソール公開鍵ペアを生成する
704 CA秘密鍵で署名されたコンソール証明書を生成する
706 コンソール秘密鍵、コンソール証明書、およびCA証明書をコンソールメモリの中に記憶する
コンソール(i)
650
CA
CA
MFG CAシステム
コンソール
Kca_prv
102(i)
メモリ
Ki_prv
コンソール
CA

【図８】


800
802 コンソール、CA証明書、およびコンソール秘密鍵の証拠を送る
804 データセンタにおいてルート公開鍵を使用してCA証明書を検証する
806 CA証明書から獲得されたCA公開鍵を使用してコンソール証明書を検証する
808 コンソール証明書から獲得されたコンソール公開鍵を使用してコンソールによってサブミットされたコンソール秘密鍵の証拠を評価する
102(i)
メモリ
Ki_prv
コンソール
CA
[証拠] Ki_prv
コンソール
CA
ネットワーク
302
310
MFG秘密DB
ルート
306
認証サーバ
Kroot_puv
CA
Kroot_puv
コンソール
Kca_puv
Ki_pub
{[証拠] Ki_prv}

フロントページの続き

(72)発明者　ボイド　シー．マルタラー
アメリカ合衆国　９８１０３　ワシントン州　シアトル　デンスモア　アベニュー　ノース　４３２５

審査官　深沢　正志

(56)参考文献　国際公開第０１／０８２０３７（WO，Ａ１）
米国特許第０６１６１１８５（ＵＳ，Ａ）
特表２０００－５１３９８３（ＪＰ，Ａ）
特開２００１－１９８３５０（ＪＰ，Ａ）
特開２００１－２７３２５５（ＪＰ，Ａ）
米国特許第０６１８９０９６（ＵＳ，Ｂ１）
国際公開第９８／０５６１７９（WO，Ａ１）
国際公開第００／０５１０３６（WO，Ａ１）
国際公開第０１／０８４７６８（WO，Ａ１）
国際公開第００／６２５４０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
A63F 13/12
G06F 21/00 - 21/24
G06F 12/14