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

特許第6072091号
(P6072091)

(45)発行日　平成29年2月1日(2017.2.1)　(24)登録日　平成29年1月13日(2017.1.13)

(51)Int.Cl.　　F I
*G06F 21/62 (2013.01)*　　G06F 21/62 390
*G06F 21/44 (2013.01)*　　G06F 21/44 350

請求項の数 12　外国語出願　(全 15 頁)

(21)出願番号　特願2015-6657(P2015-6657)
(22)出願日　平成27年1月16日(2015.1.16)
(65)公開番号　特開2015-143988(P2015-143988A)
(43)公開日　平成27年8月6日(2015.8.6)
審査請求日　平成27年2月20日(2015.2.20)
(31)優先権主張番号　103102096
(32)優先日　平成26年1月21日(2014.1.21)
(33)優先権主張国　台湾(TW)

(73)特許権者　509262068
周　宏建
台湾台中市南屯區永春東路１０００號之１９（１２樓）
(74)代理人　110000796
特許業務法人三枝国際特許事務所
(72)発明者　周　宏建
台湾台中市南屯區永春東路１０００號之１９（１２樓）

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】アプリケーション・プログラム用の安全なアクセス方法および安全なアクセス装置

(57)【特許請求の範囲】
【請求項１】
第1の認証データおよび第1のコントロール規則を含んでいる安全なアクセス装置(1)によってインプリメントされる、アプリケーションおよびアプリケーション・プログラム用の安全なアクセス方法であって、前記安全なアクセス装置(1)が、オペレーティングシステム(311)がロードされるメインメモリ(31)と、記憶装置(4)との間に接続され、前記オペレーティングシステム(311)が、前記記憶装置(4)の安全なエリア(41)に格納された合法なアプリケーション・プログラム・ファイル(5)を削除することまたは書き込むことができず、
前記合法なアプリケーション・プログラム・ファイル(5)をロードするために、前記オペレーティングシステム(311)が前記記憶装置(4)の前記安全なエリア(41)にアクセスし、合法なアプリケーション・プログラムとして機能するために、前記合法なアプリケーション・プログラム・ファイル(5)が前記オペレーティングシステム(311)内で実行されている場合に、前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信するステップであり、前記オペレーティングシステム(311)内で実行される前記合法なアプリケーション・プログラムが、認証対象のアプリケーション・プログラムとして機能する、ステップA)と、
前記オペレーティングシステム(311)内で実行される前記認証対象のアプリケーション・プログラムが、前記第1の認証データおよび前記第1のコントロール規則を含んでいるか否かに関する決定をなすステップB)と、

ステップB)においてなされた前記決定の結果が否定的な場合に、前記認証対象のアプリケーション・プログラムを、認証されていない違法なアプリケーション・プログラムであると識別し、前記違法なアプリケーション・プログラムに、アクセス対象装置へのアクセスを許可しないステップC)と、
によって特徴づけられる、安全なアクセス方法。
【請求項２】
前記合法なアプリケーション・プログラム・ファイル(5)が、サブアプリケーション・プログラムと、プリセットされた認証データと、プリセットされたコントロール規則とを含み、ステップA)がさらに、
前記プリセットされた認証データおよび前記プリセットされたコントロール規則に代えて、前記第1の認証データおよび前記第1のコントロール規則をそれぞれ用いるように、前記オペレーティングシステム(311)内で実行される前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信することを含むこと、によって特徴づけられる、請求項1に記載の安全なアクセス方法。
【請求項３】
前記記憶装置(4)の前記安全なエリアが、前記合法なアプリケーション・プログラム・ファイル(5)に加えて、対応するプリセットされた認証データと、対応するプリセットされたコントロール規則とを格納し、ステップA)がさらに、
前記合法なアプリケーション・プログラム・ファイル(5)と、前記プリセットされた認証データと、前記プリセットされたコントロール規則とをロードするために、前記オペレーティングシステム(311)が前記記憶装置(4)の前記安全なエリア(41)にアクセスし、前記合法なアプリケーション・プログラムとして機能するために、前記合法なアプリケーション・プログラム・ファイル(5)が前記オペレーティングシステム(311)内で実行される場合に、前記プリセットされた認証データおよび前記プリセットされたコントロール規則に代えて、前記第1の認証データおよび前記第1のコントロール規則をそれぞれ用いるように、前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信することを含むこと、によって特徴づけられる、請求項1に記載の安全なアクセス方法。
【請求項４】
ステップB)においてなされた前記決定の結果が肯定的な場合に、
前記認証対象のアプリケーション・プログラムから前記第1の認証データを受け取ることと、
前記認証対象のアプリケーション・プログラムの認証を開始することと、
前記安全なアクセス装置(1)の認証を、前記認証対象のアプリケーション・プログラムが開始することを可能にするために、前記認証対象のアプリケーション・プログラムに前記第1の認証データを送信することと、
を含む相互認証を行うステップD)と、
前記相互認証が成功裡に完了した後に、前記認証対象のアプリケーション・プログラムを前記合法なアプリケーション・プログラムであると識別し、前記第1のコントロール規則に一致する命令を、前記合法なアプリケーション・プログラムが前記安全なアクセス装置(1)に送信することを可能にするステップE)と、
前記命令に基づいて前記アクセス対象装置にアクセスし、前記合法なアプリケーション・プログラムが前記安全なアクセス装置(1)を通じて前記アクセス対象装置にアクセスすることを可能にするステップF)と、
によってさらに特徴づけられる、請求項1～3のいずれか1つによる安全なアクセス方法。
【請求項５】
ステップE)が、暗号化された命令を得て、前記暗号化された命令を前記安全なアクセス装置(1)に送信するために、前記合法なアプリケーション・プログラムの前記第1の認証データを使用して、前記合法なアプリケーション・プログラムが前記命令を暗号化することを可能にすることを含むこと、によって特徴づけられ、

前記安全なアクセス方法が、ステップE)とステップF)との間にさらに、
解読された命令を得るために、前記暗号化された命令を受け取り、前記安全なアクセス装置(1)の前記第1の認証データにしたがって、前記暗号化された命令を解読するステップG)、を含み、
ステップF)が、前記解読された命令に基づいて前記アクセス対象装置にアクセスすることを含むこと、によって特徴づけられる、請求項4に記載の安全なアクセス方法。
【請求項６】
前記第1のコントロール規則が、前記合法なアプリケーション・プログラムによって前記安全なアクセス装置(1)に送信された命令に関するアクセス規則であるワンタイムアクセス規則と、前記安全なアクセス装置(1)用および前記合法なアプリケーション・プログラム用の命令に関するコード規則であるワンタイム命令規則との少なくとも1つを含むこと、によって特徴づけられ、
前記第1のコントロール規則の前記ワンタイムアクセス規則は、前記記憶装置(4)の隠しエリアにアクセスするために、前記合法なアプリケーション・プログラムによって前記安全なアクセス装置(1)に送信される命令に関するアクセス規則を含み、前記隠しエリアは、前記オペレーティングシステム(311)によって検知、読み込みまたは書き込みすることができないこと、によって特徴づけられる、請求項1～5のいずれか1つによる安全なアクセス方法。
【請求項７】
オペレーティングシステム(311)がロードされるメインメモリ(31)と、記憶装置(4)を含むアクセス対象装置との間に接続され、前記オペレーティングシステム(311)が、前記記憶装置(4)の安全なエリア(41)内の合法なアプリケーション・プログラム・ファイル(5)を削除することまたは書き込むことができず、前記オペレーティングシステム(311)内で実行される認証対象のアプリケーション・プログラムに、前記アクセス対象装置へのアクセスを許可するか否かを決定するように構成された安全なアクセス装置(1)であって、
第1の認証データを生成するように構成された認証データ生成ユニット(11)と、
第1のコントロール規則を生成するように構成されたコントロール規則生成ユニット(12)と、
実行されたときに前記オペレーティングシステム(311)内で実行される合法なアプリケーション・プログラムとして機能する前記合法なアプリケーション・プログラム・ファイル(5)をロードするために、前記オペレーティングシステム(311)が前記記憶装置(4)の前記安全なエリア(41)にアクセスしている場合に、前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信するように構成される保護ユニット(15)であり、前記オペレーティングシステム(311)内で実行される前記合法なアプリケーション・プログラムが、前記認証対象のアプリケーション・プログラムとして機能する、保護ユニット(15)と、
前記オペレーティングシステム(311)内で実行される前記認証対象のアプリケーション・プログラムが、前記第1の認証データおよび前記第1のコントロール規則を含んでいるか否かに関する決定をなし、
前記決定の結果が否定的な場合に、前記認証対象のアプリケーション・プログラムを、認証されていない違法なアプリケーション・プログラムであると識別し、前記違法なアプリケーション・プログラムに、前記アクセス対象装置へのアクセスを許可しない、
ように構成された認証ユニット(14)と、
によって特徴づけられる、アプリケーション・プログラム用の安全なアクセス装置(1)。
【請求項８】
前記合法なアプリケーション・プログラム・ファイル(5)が、サブアプリケーション・プログラムと、プリセットされた認証データと、プリセットされたコントロール規則とを含み、前記保護ユニット(15)がさらに、
前記プリセットされた認証データおよび前記プリセットされたコントロール規則に代えて、前記第1の認証データおよび前記第1のコントロール規則をそれぞれ用いるように、前

記オペレーティングシステム(311)内で実行される前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信するように構成されること、によって特徴付けられる、請求項7に記載の安全なアクセス装置(1)。

【請求項９】

前記記憶装置(4)の前記安全なエリアが、前記合法なアプリケーション・プログラム・ファイル(5)に加えて、対応するプリセットされた認証データと、対応するプリセットされたコントロール規則とを格納し、

前記合法なアプリケーション・プログラム・ファイル(5)と、前記プリセットされた認証データと、前記プリセットされたコントロール規則とをロードするために、前記オペレーティングシステム(311)が前記記憶装置(4)の前記安全なエリア(41)にアクセスし、前記合法なアプリケーション・プログラムとして機能するために、前記合法なアプリケーション・プログラム・ファイル(5)が前記オペレーティングシステム(311)内で実行される場合に、前記保護ユニット(15)がさらに、前記プリセットされた認証データおよび前記プリセットされたコントロール規則に代えて、前記第1の認証データおよび前記第1のコントロール規則をそれぞれ用いるように、前記合法なアプリケーション・プログラムに、前記第1の認証データおよび前記第1のコントロール規則を送信するように構成されること、

によって特徴づけられる、請求項7に記載の安全なアクセス装置(1)。

【請求項１０】

処理ユニット(16)をさらに含み、

前記認証ユニット(14)によってなされた前記決定の結果が肯定的な場合に、

前記認証対象のアプリケーション・プログラムから前記第1の認証データを受け取ることと、

前記認証対象のアプリケーション・プログラムの認証を開始することと、

前記安全なアクセス装置(1)の認証を、前記認証対象のアプリケーション・プログラムが開始することを可能にするために、前記認証対象のアプリケーション・プログラムに前記第1の認証データを送信することと、

を含む相互認証を行なうように、前記認証ユニット(14)がさらに構成されること、によって特徴付けられ、

前記相互認証が成功裡に完了した後に、前記認証ユニット(14)が、前記認証対象のアプリケーション・プログラムを前記合法なアプリケーション・プログラムであると識別し、前記合法なアプリケーション・プログラムによって前記安全なアクセス装置(1)に送信される、前記第1のコントロール規則に一致する命令を受け取るために、前記処理ユニット(16)を活性化すること、によって特徴づけられ、

前記命令に基づいて前記アクセス対象装置にアクセスし、前記合法なアプリケーション・プログラムが前記処理ユニット(16)を通じて前記アクセス対象装置にアクセスすることを可能にするように、前記処理ユニット(16)が構成される、請求項7～9のいずれか1つによる安全なアクセス装置(1)。

【請求項１１】

暗号化された命令を得て、前記暗号化された命令を前記安全なアクセス装置(1)に送信するために、前記合法なアプリケーション・プログラムの前記第1の認証データを使用して、前記合法なアプリケーション・プログラムが前記命令を暗号化することを可能にすること、によって前記安全なアクセス装置(1)が特徴づけられ、

前記処理ユニット(16)が、解読された命令を得て、前記解読された命令に基づいて前記アクセス対象装置にアクセスするために、前記暗号化された命令を受け取り、前記認証データ生成ユニット(11)によって生成された前記第1の認証データにしたがって、前記暗号化された命令を解読すること、によって特徴付けられる、請求項10に記載の安全なアクセス装置(1)。

【請求項１２】

第1のコントロール規則が、前記合法なアプリケーション・プログラムによって前記処理ユニット(16)に送信された命令に関するアクセス規則であるワンタイムアクセス規則と

、前記処理ユニット(16)用および前記合法なアプリケーション・プログラム用の命令に関するコード規則であるワンタイム命令規則との少なくとも1つを含むこと、によって特徴づけられ、

前記第1のコントロール規則の前記ワンタイムアクセス規則は、前記記憶装置(4)の隠しエリア(42)にアクセスするために、前記合法なアプリケーション・プログラムによって前記処理ユニット(16)に送信される命令に関するアクセス規則を含み、前記隠しエリア(42)は、前記オペレーティングシステム(311)によって検知、読み込みまたは書き込みすることができないこと、によって特徴づけられる、請求項10および11の1つによる安全なアクセス装置(1)。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、アプリケーション・プログラム用の安全なアクセス方法および安全なアクセス装置に関し、より詳細には、違法な（illegitimate）アプリケーション・プログラムがアクセス対象装置（to-be-accessed device）にアクセスするのを防ぐようにするための、アクセス対象装置のアプリケーション・プログラムによる安全なアクセスのための方法および装置に関する。

【背景技術】

【０００２】

今日における情報技術の急速な発展および大衆化により、それに呼応してあらゆる種類の便利なアプリケーション・プログラムがもたらされた。たとえアプリケーション・プログラムまたはその供給者のユーザであっても、そのアプリケーション・プログラムによって提供されるサービス用の十分なセキュリティ対策があるか否かは、常に重要な関心事であった。攻撃者がアプリケーション・プログラムへ悪意のあるソフトウェアを埋め込めば、ユーザによるアプリケーション・プログラムの操作中に、個人データが盗まれる可能性があり、ドキュメントが破損される可能性があり、操作スクリーンがハイジャックされる可能性がある。その結果、ユーザの重要な個人データが漏洩または破損され、回復不能な損失が引き起こされる。

【０００３】

しかしながら、アプリケーション・プログラム用の慣習的な認証方法は、アプリケーション・プログラムのインストールを許可するための認証方法のように、主としてそれについての著作権の保護用に設計されている。下記特許文献１には、アプリケーション・プログラムのオンライン認証および記録メカニズム並びにその方法が開示されている。前述の方法は、ユーザエンドプログラムにより、オンラインログインを要求するステップと、サーバエンドにより、ユーザエンドの少なくとも1つのログインを受理するステップと、異なるコンピュータへのアプリケーション・プログラムの不法な分配を防ぐように、ユーザエンドが、ユーザエンドプログラムに関連したハードウェア環境識別コードおよび認証シリアルナンバーを格納するか否かを判断するステップと、を含んでいる。前述の認証方法は、アプリケーション・プログラムの違法コピーのみを防ぐことができる。しかしながら、この認証方法は、コンピュータ内で実行されたアプリケーション・プログラムが、コピー、あるいは悪意のあるソフトウェアによる改ざんまたは埋め込みがなされたか否かを識別することができない。

【０００４】

このようにして、アプリケーション・プログラムを、重要な個人データの侵入盗および破損という結果をもたらす、悪意のあるソフトウェアによるコピー、改ざんまたは埋め込みから防ぐための方法が、克服すべき問題となっている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】台湾特許第I283119号公報

【発明の概要】
【０００６】
したがって、本発明は、違法なアプリケーション・プログラムがアクセス対象装置にアクセスするのを防ぐようにするための、アプリケーション・プログラム用の安全なアクセス方法を提供することを目的とする。
【０００７】
それゆえに、本発明のアプリケーション・プログラム用の安全なアクセス方法は、第1の認証データおよび第1のコントロール規則を含んでいる安全なアクセス装置によって実現される。安全なアクセス方法は、
オペレーティングシステム内で実行される認証対象のアプリケーション・プログラムが、第1の認証データおよび第1のコントロール規則を含んでいるか否かに関する決定をなすステップA)と、
ステップA)においてなされた決定の結果が否定的な場合に、認証対象のアプリケーション・プログラムを、認証されていない違法なアプリケーション・プログラムであると識別し、違法なアプリケーション・プログラムに、アクセス対象装置へのアクセスを許可しないステップB)とを含んでいる。
【０００８】
本発明は、違法なアプリケーション・プログラムがアクセス対象装置にアクセスするのを防ぐようにするための、アプリケーション・プログラム用の安全なアクセス装置を提供することを別の目的とする。
【０００９】
それゆえに、本発明のアプリケーション・プログラム用の安全なアクセス装置は、オペレーティングシステムがロードされるメインメモリと、アクセス対象装置との間に接続される。安全なアクセス装置は、オペレーティングシステム内で実行される認証対象のアプリケーション・プログラムに、アクセス対象装置へのアクセスを許可するか否かを決定するように構成される。安全なアクセス装置は、認証データ生成ユニットと、コントロール規則生成ユニットと、認証ユニットとを含んでいる。認証データ生成ユニットは、第1の認証データを生成するように構成される。コントロール規則生成ユニットは、第1のコントロール規則を生成するように構成される。認証ユニットは、オペレーティングシステム内で実行される認証対象のアプリケーション・プログラムが、第1の認証データおよび第1のコントロール規則を含んでいるか否かに関する決定をなすように構成される。決定の結果が否定的な場合、認証ユニットは、認証対象のアプリケーション・プログラムを、認証されていない違法なアプリケーション・プログラムであると識別し、違法なアプリケーション・プログラムに、アクセス対象装置へのアクセスを許可しない。
【００１０】
本発明の効果は、オペレーティングシステム内で実行される認証対象のアプリケーション・プログラムが、第1の認証データおよび第1のコントロール規則を含んでいるか否かに関する決定をなす安全なアクセス装置によって、第1の認証データおよび第1のコントロール規則を含んでいない違法なアプリケーション・プログラムは、アクセス対象装置へのアクセスが妨げられ、その結果、コンピュータをセキュリティの脅威から解放することができる点にある。
【００１１】
本発明の他の特徴および利点は、添付の図面を参照する以下の実施形態の詳細な説明において明白になるであろう。
【図面の簡単な説明】
【００１２】
【図１】本発明に係るアプリケーション・プログラム用の安全なアクセス装置の一実施形態を示すブロックダイヤグラムである。
【図２】本発明に係るアプリケーション・プログラム用の安全なアクセス方法の一実施形態の認証プロセスを示すフローチャートである。

【図３】本発明に係るアプリケーション・プログラム用の安全なアクセス方法の一実施形態の再認証プロセスを示すフローチャートである。
【発明を実施するための形態】
【００１３】
図1を参照すると、本発明に係るアプリケーション・プログラム用の安全なアクセス装置1の一実施形態は、アクセス対象装置へのアクセスを、認証対象のアプリケーション・プログラム（to-be-authenticated app program）に許可するか否かを判断するように構成され、これはオペレーティングシステム311において実行される。安全なアクセス装置1は、認証データ生成ユニット11と、コントロール規則生成ユニット12と、ワンタイム・ダイナミックリンク生成ユニット13と、認証ユニット14と、保護ユニット15と、処理ユニット16とを含んでいる。アプリケーション・プログラム用の安全なアクセス装置1が、ファームウェアの形態で実現される点に注目される。また、安全なアクセス装置1の実用的な実施形態はチップとすることができ、チップは、パーソナルコンピュータ(PC)、ノート型コンピュータ、タブレットコンピュータ、スマートフォン、および記憶装置と制御対象装置（to-be-controlled device）とを含んでいるコンピューティングシステムなどにインストールされる。チップがインストールされるPCのために、PCは、マザーボード3と制御対象装置2と記憶装置4とを含めた包括的なコンポーネント中に、安全なアクセス装置1を含むであろう。アプリケーション・プログラムによってアクセスされるアクセス対象装置として、制御対象装置2および記憶装置4が協力的に動作する点に注目される。
【００１４】
マザーボード3は、メインメモリ31および中央処理装置(CPU)32を含んでいる。
【００１５】
制御対象装置2は、ニアフィールド通信ユニットのような少なくとも1つの通信ユニットと、ハードディスク、フラッシュメモリ、または他の記憶素子のような記憶装置ユニットと、キーボード、コンピュータ用マウスなどのような周辺ユニットとを含んでいる。
【００１６】
認証データ生成ユニット11は、ワンタイム認証アルゴリズム、ワンタイムパスワードおよびワンタイム認証コードの少なくとも1つを含んでいる第1の認証データを生成するように構成される。
【００１７】
コントロール規則生成ユニット12は、ワンタイムアクセス規則およびワンタイム命令規則の少なくとも1つを含んでいる第1のコントロール規則を生成するように構成される。ワンタイムアクセス規則は、合法な（legit）アプリケーション・プログラムによって処理ユニット16へ送信される命令に関するアクセス規則であり、オペレーティングシステム311において実行される。例えば、ワンタイムアクセス規則は、制御対象装置2の通信ユニット、記憶装置ユニットおよび周辺ユニットにアクセスするために、処理ユニット16への命令の発行を合法なアプリケーション・プログラムに許可するか否かに関する規則であり、また、記憶装置4の安全なエリア41内に格納されたファイルの属性を変更するために、処理ユニット16への命令の発行を合法なアプリケーション・プログラムに許可するか否かに関する規則であり、また、記憶装置4の隠しエリア42にアクセスするために、合法なアプリケーション・プログラムによって処理ユニット16へ送信される命令に関するアクセス規則である。とりわけ隠しエリア42は、オペレーティングシステム311によって検知することができず、読み込みまたは書き込みすることができない。ワンタイム命令規則は、処理ユニット16および合法なアプリケーション・プログラム用の命令に関するコード規則である。例えば、ワンタイム命令規則は、合法なアプリケーション・プログラムと処理ユニット16との間の命令コードを定義し、例えば0000は読み込み命令を表し、0001は書き込み命令を表す。異なる合法なアプリケーション・プログラムに応じて、認証データ生成ユニット11およびコントロール規則生成ユニット12は、異なる合法なアプリケーション・プログラムの各々について、別個の第1の認証データおよび第1のコントロール規則を生成することができる点に注目される。

【００１８】
ワンタイム・ダイナミックリンク生成ユニット13は、第1の認証データおよび第1のコントロール規則に基づいて、第1のワンタイム・ダイナミックリンク・プログラムを生成するように構成される。第1のワンタイム・ダイナミックリンク・プログラムは、オペレーティングシステム311によって直接実行することが可能なプログラムである。本実施形態では、合法なアプリケーション・プログラムに続いて提供される第1のワンタイム・ダイナミックリンク・プログラムに、第1の認証データおよび第1のコントロール規則を組み込むように、ワンタイム・ダイナミックリンク生成ユニット13が構成される点に注目される。第1のワンタイム・ダイナミックリンク・プログラムを受け取った後、合法なアプリケーション・プログラムは、第1のワンタイム・ダイナミックリンク・プログラムに基づいて、第1の認証データおよび第1のコントロール規則を生成する。しかしながら、本実施形態の変形例では、第1の認証データおよび第1のコントロール規則は、第1のワンタイム・ダイナミックリンク・プログラムから離れた別々のやり方において、すなわち、第1の認証データおよび第1のコントロール規則を第1のワンタイム・ダイナミックリンク・プログラムと組み合わせることなく、合法なアプリケーション・プログラムに提供されてもよく、同様の提供方法はこの開示に制限されない。

【００１９】
制御対象装置2とオペレーティングシステム311がロードされるメインメモリ31との間に接続された安全なアクセス装置1を用いて、オペレーティングシステム311内で実行された認証対象のアプリケーション・プログラムは、制御対象装置2をコントロールするように、安全なアクセス装置1の認証ユニット14を用いて相互認証を完了することが要求される。オペレーティングシステム311内で実行された合法なアプリケーション・プログラムが、アクセス対象装置にアクセスしようとする場合、合法なアプリケーション・プログラムは、安全なアクセス装置1によって認証されることが要求され、それにより、オペレーティングシステム311内で実行された認証対象のアプリケーション・プログラムとして動作する点に注目される。認証ユニット14の詳細な動作および認証プロセスが以下で述べられる。

【００２０】
認証ユニット14は、オペレーティングシステム311内で実行された認証対象のアプリケーション・プログラムが、第1の認証データおよび第1のコントロール規則を含んでいるか否かに関する決定をなすように構成される。このようになされた決定の結果が否定的な場合、それは、認証対象のアプリケーション・プログラムが認証されていない違法なアプリケーション・プログラムであることを意味し、認証ユニット14は、違法なアプリケーション・プログラムが制御対象装置2をコントロールすることを許可しない。このようになされた決定の結果が肯定的な場合、相互認証が行なわれる。具体的には、認証ユニット14が、認証対象のアプリケーション・プログラムから第1の認証データを受け取り、認証対象のアプリケーション・プログラムの認証を開始する。一方で、認証ユニット14が、認証データ生成ユニット11によって生成された第1の認証データを、認証対象のアプリケーション・プログラムに送信し、認証対象のアプリケーション・プログラムが認証データをそこから受け取り、安全なアクセス装置1の認証を開始する。

【００２１】
認証ユニット14および認証対象のアプリケーション・プログラムが、それらの間で相互認証を完了する場合、それは、認証対象のアプリケーション・プログラムが、合法なアプリケーション・プログラム・ファイル5に相当する合法なアプリケーション・プログラムであることを意味し、安全なアクセス装置1が、認証対象のアプリケーション・プログラムを合法なアプリケーション・プログラムであると識別することを意味する。合法なアプリケーション・プログラムは、暗号化された命令を得るための、合法なアプリケーション・プログラムの第1の認証データを使用して、第1のコントロール規則に一致する命令を暗号化し、暗号化された命令を処理ユニット16に送信する。処理ユニット16が暗号化された命令を受け取り、認証データ生成ユニット11によって生成される第1の認証データにした

がって、暗号化された命令を解読し、解読された命令を得るように、認証ユニット14は処理ユニット16を活性化する。続いて、合法なアプリケーション・プログラムが処理ユニット16を通じて制御対象装置2をコントロールする結果を達成するように、処理ユニット16は、解読された命令に基づいて制御対象装置2をコントロールする。言いかえれば、たとえ相互認証が完了していたとしても、オペレーティングシステム311内で実行された合法なアプリケーション・プログラムは、制御対象装置2を直接コントロールすることができない。合法なアプリケーション・プログラムは、依然として、安全なアクセス装置1の処理ユニット16を通じて制御対象装置2をコントロールすることが要求される。

【００２２】

さらに、実行用の合法なアプリケーション・プログラム・ファイル5をロードするように、オペレーティングシステム311が記憶装置4の安全なエリア41にアクセスしようとする場合、記憶装置4とオペレーティングシステム311がロードされるメインメモリ31との間に安全なアクセス装置1が接続されるので、オペレーティングシステム311は、安全なアクセス装置1を通じて合法なアプリケーション・プログラム・ファイル5をロードすることが要求される。合法なアプリケーション・プログラム・ファイル5は、メインメモリ31にロードされ、合法なアプリケーション・プログラムとして機能するために、CPU 32によってオペレーティングシステム311内で実行される。さらに、安全なアクセス装置1の保護ユニット15は、合法なアプリケーション・プログラムに第1のワンタイム・ダイナミックリンク・プログラムを供給するように構成される。保護ユニット15の詳細な動作が以下で説明される。

【００２３】

オペレーティングシステム311が、共に安全なエリア41内に格納されている、ダイナミックリンク・ライブラリ(DLL)ファイルのような合法なアプリケーション・プログラム・ファイル5と、対応するプリセットされたワンタイム・ダイナミックリンク・プログラムとをロードするように、記憶装置4の安全なエリア41にアクセスし、合法なアプリケーション・プログラムとして機能するように、合法なアプリケーション・プログラム・ファイル5が、ロードされた後にオペレーティングシステム311によって実行されている場合、保護ユニット15は、オペレーティングシステム311内で実行されている合法なアプリケーション・プログラムに、第1のワンタイム・ダイナミックリンク・プログラムを送信するように構成され、プリセットされたワンタイム・ダイナミックリンク・プログラムに代えて、第1のワンタイム・ダイナミックリンク・プログラムが用いられる。オペレーティングシステム311は、安全なエリア41内に格納された合法なアプリケーション・プログラム・ファイル5を削除することまたは書き込むことができない。本実施形態では、合法なアプリケーション・プログラム・ファイル5およびプリセットされたワンタイム・ダイナミックリンク・プログラムは、２つの個別のファイルである。オペレーティングシステム311は、合法なアプリケーション・プログラムおよび第1のワンタイム・ダイナミックリンク・プログラムを個別に読み込むように構成、すなわち、合法なアプリケーション・プログラムを最初に読み込み、次に、プリセットされたワンタイム・ダイナミックリンク・プログラムと交換する予定である、第1のワンタイム・ダイナミックリンク・プログラムを読み込むように構成されている。しかしながら、別の実施形態では、合法なアプリケーション・プログラム・ファイル5と対応するプリセットされたワンタイム・ダイナミックリンク・プログラムとは、単一のファイルに属していてもよい。すなわち、合法なアプリケーション・プログラム・ファイル5は、合法なアプリケーション・プログラムおよびプリセットされたワンタイム・ダイナミックリンク・プログラムに相当するサブアプリケーション・プログラムを含んでいる。このように、オペレーティングシステム311は、合法なアプリケーション・プログラムおよび第1のワンタイム・ダイナミックリンクプログラムを個別に読み込むことができず、サブアプリケーション・プログラムおよび第1のワンタイム・ダイナミックリンク・プログラムを含んでいる合法なアプリケーション・プログラムを読み込むように、プリセットされたワンタイム・ダイナミックリンク・プログラムが第1のワンタイム・ダイナミックリンク・プログラムに取り替えられるまで、待機すること

が必要とされる。具体的には、プリセットされたワンタイム・ダイナミックリンク・プログラムは、プリセットされた認証データおよびプリセットされたコントロール規則を含み、プリセットされた認証データおよびプリセットされたコントロール規則に代えて、第1の認証データおよび第1のコントロール規則がそれぞれ用いられるように、保護ユニット15が合法なアプリケーション・プログラムに第1の認証データおよび第1のコントロール規則をそれぞれ送信する。

【００２４】

認証ユニット14および認証対象のアプリケーション・プログラムが認証をもう一度行うこと、すなわち再認証プロセスが要求される場合、認証データ生成ユニット11は、第2の認証データを生成するようにさらに構成され、コントロール規則生成ユニット12は、第2のコントロール規則を生成するようにさらに構成される。具体的には、第2の認証データは、別のワンタイム認証アルゴリズム、別のワンタイムパスワードおよび別のワンタイム認証コードの少なくとも1つを含んでいる。第2のコントロール規則は、別のワンタイムアクセス規則および別のワンタイム命令規則の少なくとも1つを含んでいる。ワンタイム・ダイナミックリンク生成ユニット13は、第2の認証データおよび第2のコントロール規則に基づいて、第2のワンタイム・ダイナミックリンク・プログラムを生成するようにさらに構成される。第1の認証データおよび第1のコントロール規則に代えて、第2の認証データおよび第2のコントロール規則がそれぞれ用いられるように、保護ユニット15は、オペレーティングシステム311内で実行されている合法なアプリケーション・プログラムに、第2のワンタイム・ダイナミックリンク・プログラムを送信するように構成される。この瞬間では、合法なアプリケーション・プログラムは、認証対象のアプリケーション・プログラムとしてもう一度機能する。したがって、認証ユニット14は、認証対象のアプリケーション・プログラムから第2の認証データを受け取り、認証対象のアプリケーション・プログラムの認証をもう一度開始する。その間に、認証対象のアプリケーション・プログラムは、認証ユニット14から第2の認証データを受け取り、認証ユニット14の認証をもう一度開始する。

【００２５】

図2および図3を参照して、本発明に係るアプリケーション・プログラム用の安全なアクセス方法の一実施形態が示される。安全なアクセス方法は、安全なアクセス装置1によって実現され、認証プロセスおよび再認証プロセスを含んでいる。

【００２６】

図1および図2を参照すると、本発明に係る安全なアクセス方法は次のステップを含んでいる。

【００２７】

ステップ601において、合法なアプリケーション・プログラムとしてオペレーティングシステム311上で実行される合法なアプリケーション・プログラム・ファイル5と、対応するプリセットされたワンタイム・ダイナミックリンク・プログラムとをロードするために、オペレーティングシステム311が、安全なアクセス装置1を通じて記憶装置4の安全なエリア41にアクセスしている場合、認証データ生成ユニット11は第1の認証データを生成し、コントロール規則生成ユニット12は第1のコントロール規則を生成し、ワンタイム・ダイナミックリンク生成ユニット13は、第1の認証データおよび第1のコントロール規則に基づいて第1のワンタイム・ダイナミックリンク・プログラムを生成する。保護ユニット15は、プリセットされたワンタイム・ダイナミックリンク・プログラムに代えて用いるために、オペレーティングシステム311内で実行されている合法なアプリケーション・プログラムに、第1のワンタイム・ダイナミックリンク・プログラムを送信する。

【００２８】

ステップ602において、合法なアプリケーション・プログラムは、第1のワンタイム・ダイナミックリンク・プログラムに基づいて、第1の認証データおよび第1のコントロール規則を生成する。

【００２９】

オペレーティングシステム311にセキュリティ上の欠陥が存在する可能性があるので、合法なアプリケーション・プログラムは、合法なアプリケーション・プログラムをオペレーティングシステム311にロードする過程の間のまたは合法なアプリケーション・プログラムをオペレーティングシステム311上で実行する過程の間の改ざんに弱い点に注目される。したがって、オペレーティングシステム311内で実行されるアプリケーション・プログラムは、アクセス対象装置にアクセスするように、制御対象装置2をコントロールするように認証されることが要求される。オペレーティングシステム311内でこのように実行されたアプリケーション・プログラムは、認証対象のアプリケーション・プログラムとして機能する。

【００３０】

ステップ603において、認証ユニット14は、オペレーティングシステム311内で実行された認証対象のアプリケーション・プログラムが、第1の認証データおよび第1のコントロール規則を備えているか否かに関する決定をなす。

【００３１】

ステップ604において、ステップ603においてなされた決定の結果が否定的な場合、それは、安全なアクセス装置1が、認証対象のアプリケーション・プログラムを認証されていない違法なアプリケーション・プログラムであると識別し、それにより、違法なアプリケーション・プログラムがアクセス対象装置にアクセスすることを許可しないことを意味する。

【００３２】

ステップ605において、ステップ603においてなされた決定の結果が肯定的な場合、相互認証が行なわれる。具体的には、認証ユニット14が、認証対象のアプリケーション・プログラムから第1の認証データを受け取り、認証対象のアプリケーション・プログラムの認証を開始し、認証対象のアプリケーション・プログラムが、認証ユニット14から第1の認証データを受け取り、安全なアクセス装置1の認証ユニット14の認証を開始する。認証対象のアプリケーション・プログラムによって認証ユニット14から受け取った第1の認証データは、認証データ生成ユニット11によって生成された第1の認証データである。

【００３３】

一旦、認証ユニット14および認証対象のアプリケーション・プログラムが、認証対象のアプリケーション・プログラムが合法なアプリケーション・プログラム5であると識別されることを意味する両者の間の前述の相互認証を成功裡に完了したならば、プロセスはステップ606に移る。ステップ606において、合法なアプリケーション・プログラムは、暗号化された命令を得るための、合法なアプリケーション・プログラムの第1の認証データを使用して、第1のコントロール規則に一致する命令を暗号化し、暗号化された命令を処理ユニット16に送信する。

【００３４】

ステップ607において、処理ユニット16が暗号化された命令を受け取り、認証データ生成ユニット11によって生成される第1の認証データにしたがって、暗号化された命令を解読し、解読された命令を得るように、認証ユニット14は処理ユニット16を活性化する。

【００３５】

ステップ608において、処理ユニット16は、解読された命令に基づいてアクセス対象装置にアクセスする。その結果、合法なアプリケーション・プログラムは、処理ユニット16を通じて制御対象装置2をコントロールするように、アクセス対象装置にアクセスすることができる。

【００３６】

図1および図3を参照すると、本発明に係る安全なアクセス方法の再認証プロセスのステップが示される。再認証プロセスが必要とされる複数の状況が存在する。例えば、或るシナリオでは、合法なアプリケーション・プログラムが制御対象装置2をコントロールする命令をもう一度送信しようとする場合は常に、再認証プロセスがコールされる。別のシナリオでは、合法なアプリケーション・プログラムが制御対象装置2をコントロールする特

定の命令を送信しようとする場合に限り、再認証プロセスがコールされる。また別のシナリオでは、再認証プロセスは所定の時間周期毎にコールされる。再認証プロセスがコールされる異なる状況は、異なるニーズにしたがって設定することができる。再認証プロセスは、合法なアプリケーション・プログラムが、違法なアプリケーション・プログラムになると気付かれていないものに取り替えられまたは改ざんされ、それによって、再認証プロセスが行なわれなければ違法なアプリケーション・プログラムがアクセス対象装置へのアクセスを獲得するであろう状況を、防ぐことができる。さらに、再認証プロセスは、安全なアクセス装置1と合法なアプリケーション・プログラム5との間のコントロール規則に変更を行うことを可能にする。再認証プロセスのステップに関連した詳細な記述は以下に提供される。

【００３７】

ステップ701において、認証データ生成ユニット11は第2の認証データを生成し、コントロール規則生成ユニット12は第2のコントロール規則を生成し、ワンタイム・ダイナミックリンク生成ユニット13は、第2の認証データおよび第2のコントロール規則に基づいて、第2のワンタイム・ダイナミックリンク・プログラムを生成する。保護ユニット15は、第1のワンタイム・ダイナミックリンク・プログラムに代えて用いるために、オペレーティングシステム311内で実行されている合法なアプリケーション・プログラムに、第2のワンタイム・ダイナミックリンク・プログラムを送信する。

【００３８】

ステップ702において、合法なアプリケーション・プログラムは、第2のワンタイム・ダイナミックリンク・プログラムに基づいて、第2の認証データおよび第2のコントロール規則を生成する。

【００３９】

オペレーティングシステム311内で実行されるアプリケーション・プログラムは、アクセス対象装置にもう一度アクセスするように、制御対象装置2を再びコントロールするように再認証されることが要求されるので、オペレーティングシステム311内でこのように実行されたアプリケーション・プログラムは、認証対象のアプリケーション・プログラムとして機能する、という点に注目される。

【００４０】

ステップ703において、認証ユニット14は、オペレーティングシステム311内で実行された認証対象のアプリケーション・プログラムが、第2の認証データおよび第2のコントロール規則を備えているか否かに関する別の決定をなす。

【００４１】

ステップ704において、ステップ703においてなされた別の決定の結果が否定的な場合、それは、安全なアクセス装置1が、認証対象のアプリケーション・プログラムを認証されていない違法なアプリケーション・プログラムであると識別し、それにより、違法なアプリケーション・プログラムがアクセス対象装置にアクセスすることを許可しないことを意味する。

【００４２】

ステップ705において、ステップ703においてなされた別の決定の結果が肯定的な場合、相互認証が行なわれる。具体的には、認証ユニット14が、認証対象のアプリケーション・プログラムから第2の認証データを受け取り、認証対象のアプリケーション・プログラムの認証を開始し、認証対象のアプリケーション・プログラムが、認証ユニット14から第2の認証データを受け取り、安全なアクセス装置1の認証ユニット14の認証を開始する。認証対象のアプリケーション・プログラムによって認証ユニット14から受け取った第2の認証データは、認証データ生成ユニット11によって生成された第2の認証データである。

【００４３】

認証ユニット14および認証対象のアプリケーション・プログラムが、認証対象のアプリケーション・プログラムが合法なアプリケーション・プログラム5であると識別されることを意味する両者の間の前述の相互認証を成功裡に完了した後、プロセスはステップ706

に移る。ステップ706において、合法なアプリケーション・プログラムは、別の暗号化された命令を得るための、合法なアプリケーション・プログラムの第2の認証データを使用して、第2のコントロール規則に一致する別の命令を暗号化し、別の暗号化された命令を処理ユニット16に送信する。

【００４４】

ステップ707において、処理ユニット16が別の暗号化された命令を受け取り、認証データ生成ユニット11によって生成される第2の認証データにしたがって、別の暗号化された命令を解読し、別の解読された命令を得るように、認証ユニット14は処理ユニット16を活性化する。

【００４５】

ステップ708において、処理ユニット16は、別の解読された命令に基づいてアクセス対象装置にアクセスする。その結果、合法なアプリケーション・プログラムは、処理ユニット16を通じて制御対象装置2をコントロールするように、アクセス対象装置にアクセスすることができる。

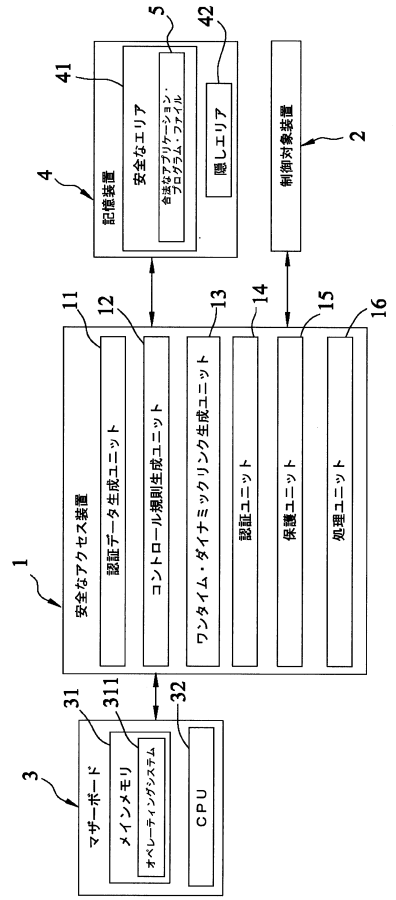
【００４６】

要約すると、記憶装置4の安全なエリア41内に合法なアプリケーション・プログラム・ファイル5を格納することにより、オペレーティングシステム311も悪意のあるソフトウェアいずれも、安全なエリア41の合法なアプリケーション・プログラム・ファイル5を削除することまたは書き込むことができない。したがって、同様のものがコピーされ、あるいは悪意のあるソフトウェアによる改ざんまたは埋め込みがなされる可能性がある唯一の機会は、合法なアプリケーション・プログラムとしての、オペレーティングシステム311内でのその実行中である。しかしながら、オペレーティングシステム311内で実行される合法なアプリケーション・プログラムに第1のワンタイム・ダイナミックリンク・プログラムを送信する保護ユニット15によって、一旦、合法なアプリケーション・プログラムがコピー、あるいは悪意のあるソフトウェアによる改ざんまたは埋め込みがなされれば、合法なアプリケーション・プログラムは、もはや第1のワンタイム・ダイナミックリンク・プログラムを保持せず、あるいは第1のワンタイム・ダイナミックリンク・プログラムは変更され、その結果、認証対象のアプリケーション・プログラムとして機能する合法なアプリケーション・プログラムは、認証ユニット14によって合法と認証されることができない。このように、第1の認証データおよび第1のコントロール規則を備えている合法なアプリケーション・プログラム5だけが、アクセス対象装置にアクセスすることができる。

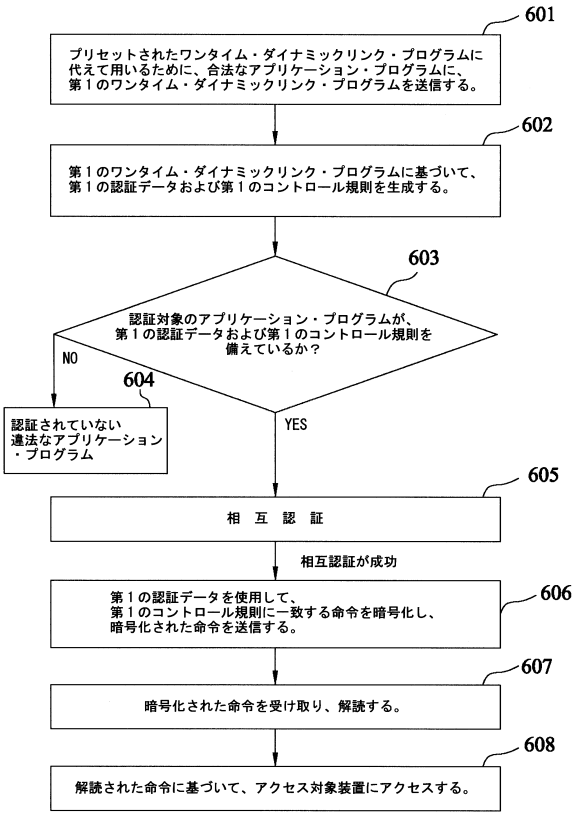
【００４７】

以上、本発明を最も実用的な実施形態と考えられるものに関して記述してきたが、本発明は、開示した実施形態に制限されることなく、同様の修正および等価な配置のすべてを包含するような、最も広い解釈の精神および範囲内に含まれる様々な配置をカバーするように意図されることが理解される。

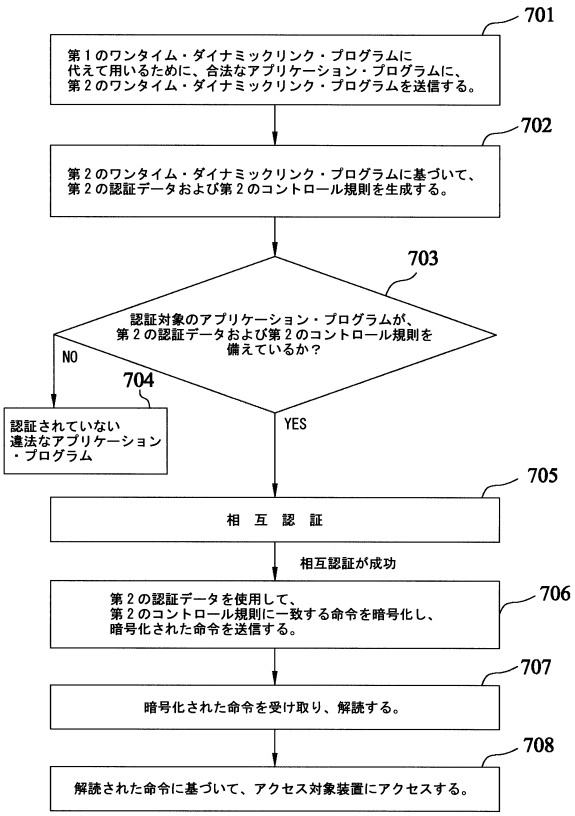
【図１】


5
42
41
安全なエリア
合法なアプリケーション・プログラム・ファイル
隠しエリア
記憶装置
4
制御対象装置
2
11
12
13
14
15
16
安全なアクセス装置
認証データ生成ユニット
コントロール規則生成ユニット
ワンタイム・ダイナミックリンク生成ユニット
認証ユニット
保護ユニット
処理ユニット
1
31
311
32
マザーボード
メインメモリ
オペレーティングシステム
CPU
3

【図２】


601
プリセットされたワンタイム・ダイナミックリンク・プログラムに代えて用いるために、合法なアプリケーション・プログラムに、第１のワンタイム・ダイナミックリンク・プログラムを送信する。
602
第１のワンタイム・ダイナミックリンク・プログラムに基づいて、第１の認証データおよび第１のコントロール規則を生成する。
603
認証対象のアプリケーション・プログラムが、第１の認証データおよび第１のコントロール規則を備えているか？
NO
604
認証されていない違法なアプリケーション・プログラム
YES
605
相 互 認 証
相互認証が成功
606
第１の認証データを使用して、第１のコントロール規則に一致する命令を暗号化し、暗号化された命令を送信する。
607
暗号化された命令を受け取り、解読する。
608
解読された命令に基づいて、アクセス対象装置にアクセスする。

【図３】


701
第１のワンタイム・ダイナミックリンク・プログラムに代えて用いるために、合法なアプリケーション・プログラムに、第２のワンタイム・ダイナミックリンク・プログラムを送信する。
702
第２のワンタイム・ダイナミックリンク・プログラムに基づいて、第２の認証データおよび第２のコントロール規則を生成する。
703
認証対象のアプリケーション・プログラムが、第２の認証データおよび第２のコントロール規則を備えているか？
NO
704
認証されていない違法なアプリケーション・プログラム
YES
705
相 互 認 証
相互認証が成功
706
第２の認証データを使用して、第２のコントロール規則に一致する命令を暗号化し、暗号化された命令を送信する。
707
暗号化された命令を受け取り、解読する。
708
解読された命令に基づいて、アクセス対象装置にアクセスする。

フロントページの続き

(56)参考文献 特開２００７－１８３９３１（ＪＰ，Ａ）
特開２０１１－０２８６８８（ＪＰ，Ａ）
特開２０１０－２２５０５５（ＪＰ，Ａ）
特開平０６－２１４９５２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０