(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第4832604号
(P4832604)
(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月30日(2011.9.30)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
G06F 21/24 (2006.01)　　G06F 15/00 330C
H04L 9/32 (2006.01)　　G06F 12/14 540A
　　H04L 9/00 673B

請求項の数 8　(全 29 頁)

(21)出願番号　特願2011-69187(P2011-69187)
(22)出願日　平成23年3月28日(2011.3.28)
審査請求日　平成23年4月27日(2011.4.27)

早期審査対象出願

(73)特許権者　000155469
株式会社野村総合研究所
東京都千代田区丸の内一丁目６番５号
(74)代理人　100096091
弁理士　井上　誠一
(74)復代理人　100155882
弁理士　齋藤　昭彦
(72)発明者　上野　正浩
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内
(72)発明者　新妻　拓朗
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

最終頁に続く

(54)【発明の名称】使用管理システムおよび使用管理方法

(57)【特許請求の範囲】
【請求項１】
端末と、前記端末と管理対象ネットワークを介して接続されるサーバとから構成され、前記端末の使用を管理する使用管理システムであって、
前記サーバは、
前記管理対象ネットワークに対して、インターネットプロトコルを利用した通信によって、前記端末の使用を許可することを示す許可情報のパケットを間欠的に同報送信する同報送信手段、
を具備し、
前記端末は、
同報送信される情報を受信する同報受信手段と、
前記同報受信手段によって前記パケットを受信したかどうかによるパケット認証を少なくとも含む、複数種類の認証処理を実行する認証処理手段と、
前記認証処理手段による各種認証処理の結果と、各認証処理について予め設定された安全指数とに基づいて端末のセキュリティレベルを判定する判定手段と、
前記判定手段により判定されたセキュリティレベルに応じて、使用できる機能を制限して自らを起動する起動手段と、
を具備することを特徴とする使用管理システム。
【請求項２】
前記管理対象ネットワークが、公衆の通信ネットワークを利用して構築される場合、

前記端末が具備する認証処理手段は、更に、
端末に割り当てられたＩＰアドレスに基づき当該端末の位置情報を取得し、使用を許可された範囲内にあるかどうかによるＩＰアドレス認証、および通信接続している基地局から送信される基地局識別情報に基づき当該端末の位置情報を取得し、使用を許可された範囲内にあるかどうかによる基地局認証のうち少なくともいずれか一方または両方を実行し、
前記パケット認証、前記ＩＰアドレス認証、および前記基地局認証のうち少なくともいずれかの認証が成功した場合に、前記判定手段によるセキュリティレベルの判定を行うことを特徴とする請求項１に記載の使用管理システム。
【請求項３】
前記端末は、前記使用可能状態において、所定時間ごとに前記認証処理を実行し、認証処理の結果に基づく前記セキュリティレベルの判定を前記判定手段により行い、所定のセキュリティレベルに達していない場合には、ユーザによって使用できない状態である使用不可能状態、或いは使用できる機能を制限した機能制限状態に自らを遷移させる監視手段、を更に具備することを特徴とする請求項１または請求項２に記載の使用管理システム。
【請求項４】
前記管理対象ネットワークが無線通信ネットワークを含む場合、
無線基地局が、前記端末の使用を許可することを示す許可情報を間欠的に同報送信する無線同報送信手段を備え、
前記端末の前記同報受信手段は、前記無線基地局から同報送信される情報を受信し、
前記認証処理手段によるパケット認証処理は、前記無線基地局から同報送信される情報も認証の対象とすることを特徴とする請求項１から請求項３のいずれかに記載の使用管理システム。
【請求項５】
前記端末が具備する認証処理手段は、更に、自らのＧＰＳ受信部によって受信される位置情報が当該端末の使用を許可する範囲内かどうかの認証であるＧＰＳ認証、自らの電波受信部によって受信される電波が当該端末の使用を許可するものかどうかの認証である電波認証、または自らの受光部によって受光される光が当該端末の使用を許可するものかどうかの認証である光認証の少なくとも１つを含むことを特徴とする請求項１から請求項４のいずれかに記載の使用管理システム。
【請求項６】
前記端末は、自らの記憶部に記憶される情報を自動的に暗号化し、かつ前記使用可能状態では復号して読み取り可能とする情報保護手段、を更に具備し、
前記端末が具備する前記同報受信手段および前記起動手段は、前記情報保護手段の一部として実行されることを特徴とする請求項１から請求項５のいずれかに記載の使用管理システム。
【請求項７】
前記端末は、予め定められたセキュリティポリシーに適合しているかどうかを検疫する検疫手段、を更に具備し、
前記検疫手段は、前記端末が具備する前記起動手段および前記監視手段の結果を収集し、前記サーバに送信することを特徴とする請求項３に記載の使用管理システム。
【請求項８】
端末と、前記端末と管理対象ネットワークを介して接続されるサーバとによって実行され、前記端末の使用を管理する使用管理方法であって、
前記サーバは、
前記管理対象ネットワークに対して、インターネットプロトコルを利用した通信によって、前記端末の使用を許可することを示す許可情報のパケットを間欠的に同報送信し、
前記端末は、
同報送信される情報を受信し、
前記パケットを受信したかどうかによるパケット認証を含む、複数種類の認証処理を実

行し、
各種認証処理の結果と、各認証処理について予め設定された安全指数とに基づいて端末のセキュリティレベルを判定し、
判定されたセキュリティレベルに応じて、使用できる機能を制限して自らを起動することを特徴とする使用管理方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータの使用を適切に管理する使用管理システム等に関するものである。
【背景技術】
【０００２】
企業等では、社員一人一人に一台のコンピュータを配布することが多い。営業秘密や個人情報などの情報漏洩を防止するため、通常、コンピュータの使用は、企業等の施設内に限られる。
しかしながら、ノート型ＰＣ（パーソナルコンピュータ）など容易に持ち運びが出来るコンピュータの場合、社員は自宅などに持ち帰ってしまうことがある。社員の自宅などでは、企業等の施設内にて使用される場合のセキュリティポリシーを適用することができないことから、不正目的の使用を防ぐことができない。また、社員には不正目的の意思がなくても、盗難や紛失などが発生すれば、第三者によって不正目的の使用が行われてしまう。
そこで、企業等の施設外では、コンピュータの使用を制限するための仕組みが望まれる。
【０００３】
特許文献１では、ＲＦＩＤを利用した情報処理端末のセキュリティ管理システムが開示されている。特許文献１の段落００２７には、会社の社内等のネットワークのセキュリティ保護が適切に行われている場所では、卓上等に設置されたＲＦＩＤ発信機から利用場所の情報を取得し、情報処理端末の利用時の認証を行うことが記載されている。また、社外に持ち出した際にはＲＦＩＤ発信機から情報を取得できないので、認証を行うことができないことが記載されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００９－２３７９０５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、ＲＦＩＤ受信機能は、通常のコンピュータには搭載されていない為、ＲＦＩＤ受信機能を有するコンピュータを購入する必要がある。また、会社等の施設が広い場合、多くのＲＦＩＤ発信機を設置する必要がある。そうすると、数多くの社員を有する企業においては、特許文献１に記載のシステムを導入することはコストの面で現実的ではない。
また、特許文献１に記載の仕組みだけでは、ＲＦＩＤ受信機能を有さないコンピュータを使用したいときに認証を行うことができず、不便である。
【０００６】
本発明は、前述した問題点に鑑みてなされたもので、その目的とすることは、コストをかけず、確実に使用を管理することが可能な使用管理システム等を提供することである。また、その他の目的は、様々な認証の仕組みを備え、利便性の高い使用管理システム等を提供することである。

【課題を解決するための手段】
【０００７】
前述した目的を達成するために第１の発明は、端末と、前記端末と管理対象ネットワークを介して接続されるサーバとから構成され、前記端末の使用を管理する使用管理システムであって、前記サーバは、前記管理対象ネットワークに対して、インターネットプロトコルを利用した通信によって、前記端末の使用を許可することを示す許可情報のパケットを間欠的に同報送信する同報送信手段、を具備し、前記端末は、同報送信される情報を受信する同報受信手段と、前記同報受信手段によって前記パケットを受信したかどうかによるパケット認証を少なくとも含む、複数種類の認証処理を実行する認証処理手段と、前記認証処理手段による各種認証処理の結果と、各認証処理について予め設定された安全指数とに基づいて端末のセキュリティレベルを判定する判定手段と、前記判定手段により判定されたセキュリティレベルに応じて、使用できる機能を制限して自らを起動する起動手段と、を具備することを特徴とする使用管理システムである。
第１の発明によって、管理対象ネットワークに接続していない状態で端末の使用を試みても、端末を使用することはできないので、管理主体の施設外での不正使用を防止することができる。また、複数の認証処理を組み合わせて実行することでセキュリティレベルをより細かく判定し、各レベルに応じた使用制限をすることが可能となり、柔軟なセキュリティ管理を行える。

【０００８】
第１の発明において、前記管理対象ネットワークが、公衆の通信ネットワークを利用して構築される場合、前記端末が具備する認証処理手段は、更に、端末に割り当てられたＩＰアドレスに基づき当該端末の位置情報を取得し、使用を許可された範囲内にあるかどうかによるＩＰアドレス認証、および通信接続している基地局から送信される基地局識別情報に基づき当該端末の位置情報を取得し、使用を許可された範囲内にあるかどうかによる基地局認証のうち少なくともいずれか一方または両方を実行し、前記パケット認証、前記ＩＰアドレス認証、および前記基地局認証のうち少なくともいずれかの認証が成功した場合に、前記判定手段によるセキュリティレベルの判定を行うことが望ましい。
これによって、端末を管理主体の施設外に持出し、インターネット等の公衆のネットワークに接続した場合であっても、ＩＰアドレスや基地局の識別情報から端末の位置を割り出して端末の使用を制限または許可できるため、管理対象ネットワークの拡張を低コストに実現できる。また、より柔軟なセキュリティ管理を行える。
【０００９】
また、第１の発明において、前記端末は、前記使用可能状態において、所定時間ごとに前記認証処理を実行し、認証処理の結果に基づく前記セキュリティレベルの判定を前記判定手段により行い、所定のセキュリティレベルに達していない場合には、ユーザによって使用できない状態である使用不可能状態、或いは使用できる機能を制限した機能制限状態に自らを遷移させる監視手段、を更に具備することが望ましい。
使用可能状態で端末が管理主体の施設外に持ち運ばれても、端末をそのまま使用することを防止することができる。また、使用可能状態では、端末は管理対象ネットワークに接続されていることになるので、ユーザがセキュリティポリシーを守っているか否かをリアルタイムで監視することもできる。
【００１０】
また、第１の発明において、前記管理対象ネットワークが無線通信ネットワークを含む場合、無線基地局が、前記端末の使用を許可することを示す許可情報を間欠的に同報送信する無線同報送信手段を備え、前記端末の前記同報受信手段は、前記無線基地局から同報送信される情報を受信し、前記認証処理手段によるパケット認証処理は、前記無線基地局から同報送信される情報も認証の対象とすることが望ましい。
これによって、端末は無線基地局から同報送信される許可情報を受信して、パケット認証を行えるため、モバイル端末を利用した使用管理システムの構築に好適である。

【００１１】
また、第１の発明における前記端末が具備する認証処理手段は、更に、自らのＧＰＳ受信部によって受信される位置情報が当該端末の使用を許可する範囲内かどうかの認証であるＧＰＳ認証、自らの電波受信部によって受信される電波が当該端末の使用を許可するものかどうかの認証である電波認証、または自らの受光部によって受光される光が当該端末の使用を許可するものかどうかの認証である光認証の少なくとも１つを含むことが望ましい。
これによって、端末のハードウエア構成や使用する環境に適した認証を行うことができ、利便性を高めることができる。特に、様々な認証の仕組みを備えることで、設備に応じた柔軟なセキュリティ管理を行える。
【００１２】
また、第１の発明における前記端末は、例えば、自らの記憶部に記憶される情報を自動的に暗号化し、かつ前記使用可能状態では復号して読み取り可能とする情報保護手段、を更に具備し、前記端末が具備する前記同報受信手段および前記起動手段は、前記情報保護手段の一部として実行される。
これによって、仮に記憶部を取り外して、記憶部の解析を試みても、情報を読み取ることはできない。
【００１３】
また、第１の発明における前記端末は、例えば、予め定められたセキュリティポリシーに適合しているかどうかを検疫する検疫手段、を更に具備し、前記検疫手段は、前記端末が具備する前記起動手段および前記監視手段の結果を収集し、前記サーバに送信する。
これによって、万が一不正使用が行われた場合であっても、不正使用後に端末が管理対象ネットワークに接続されることで、不正使用の履歴を追跡することができる。
【００１４】
第２の発明は、端末と、前記端末と管理対象ネットワークを介して接続されるサーバとによって実行され、前記端末の使用を管理する使用管理方法であって、前記サーバは、前記管理対象ネットワークに対して、インターネットプロトコルを利用した通信によって、前記端末の使用を許可することを示す許可情報のパケットを間欠的に同報送信し、前記端末は、同報送信される情報を受信し、前記パケットを受信したかどうかによるパケット認証を含む、複数種類の認証処理を実行し、各種認証処理の結果と、各認証処理について予め設定された安全指数とに基づいて端末のセキュリティレベルを判定し、判定されたセキュリティレベルに応じて、使用できる機能を制限して自らを起動することを特徴とする使用管理方法である。
第２の発明によって、管理対象ネットワークに接続していない状態で端末の使用を試みても、端末を使用することはできないので、管理主体の施設外での不正使用を防止することができる。また、複数の認証処理を組み合わせて実行することでセキュリティレベルをより細かく判定し、各レベルに応じた使用制限をすることが可能となり、柔軟なセキュリティ管理を行える。
【発明の効果】
【００１５】
本発明により、コストをかけず、確実に使用を管理することが可能な使用管理システム等を提供することができる。また、様々な認証の仕組みを備え、利便性の高い使用管理システム等を提供することができる。
【図面の簡単な説明】
【００１６】
【図１】第１の実施の形態における使用管理システム１の全体構成図
【図２】サーバ３および端末５を実現するコンピュータのハードウエア構成図
【図３】サーバ３の記憶部１２に記憶されるプログラムの一例を示す図
【図４】第１の実施の形態における端末５の記憶部１２に記憶されるプログラムの一例を示す図

【図５】第１の実施の形態における端末５の起動処理の詳細を示すフローチャート
【図６】第１の実施の形態における端末５の監視処理の詳細を示すフローチャート
【図７】第２の実施の形態における端末５の記憶部１２に記憶されるプログラムの一例を示す図
【図８】第３の実施の形態における使用管理システム１ａの全体構成図
【図９】第３の実施の形態における端末５ａを実現するコンピュータのハードウエア構成図
【図１０】第３の実施の形態における端末５ａの記憶部１２に記憶されるプログラムの一例を示す図
【図１１】セキュリティレベル表６１の一例を示す図
【図１２】第３の実施の形態における端末５ａの起動処理の詳細を示すフローチャート
【図１３】第３の実施の形態における端末５ａの監視処理の詳細を示すフローチャート
【図１４】第４の実施の形態における端末５ｂの記憶部１２に記憶されるプログラムの一例を示す図
【図１５】安全指数表２１の一例を示す図
【図１６】レベル別起動設定２２の一例を示す図
【図１７】第４の実施の形態における端末５ｂの起動処理の詳細を示すフローチャート
【図１８】第４の実施の形態のセキュリティレベル算出例を説明する図
【図１９】第４の実施の形態における端末５ｂの監視処理の詳細を示すフローチャート
【図２０】第５の実施の形態における使用管理システム１ｃの全体構成図
【図２１】第５の実施の形態における端末５ｃを実現するコンピュータのハードウエア構成図
【図２２】第５の実施の形態における端末５ｃの記憶部１２に記憶されるプログラムの一例
【図２３】第５の実施の形態で適用される安全指数表２５の一例を示す図
【図２４】第５の実施の形態における端末５ｃの起動処理の詳細を示すフローチャート
【図２５】第５の実施の形態のセキュリティレベル算出例を説明する図
【図２６】第５の実施の形態における端末５ｃの監視処理の詳細を示すフローチャート
【図２７】第５の実施の形態における端末５ｃの記憶部１２に記憶されるプログラムの一例を示す図

【発明を実施するための形態】

【００１７】

以下図面に基づいて、本発明の実施形態を詳細に説明する。

＜第１の実施の形態＞

図１は、第１の実施の形態における使用管理システム１の全体構成図である。使用管理システム１では、管理対象ネットワーク２に接続される端末５（コンピュータ）の使用を管理する。

管理対象ネットワーク２は、企業等の単一の管理主体によって管理され、インターネット等の外部ネットワークに対して閉じているネットワークである。管理対象ネットワーク２は、例えば、企業等の社内ＬＡＮ(Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ)、複数の拠点に敷設されているＬＡＮが専用線等によって接続される社内ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等が挙げられる。

管理対象ネットワーク２に用いられる物理的な各種のネットワーク機器は、外部の者が利用できない場所（例えば、管理主体が企業であれば企業の施設内）のみに設置される。従って、外部の者は、管理対象ネットワーク２に端末５を接続することができない。

尚、図１には、ネットワーク機器の一例としてルータ４を図示しているが、ネットワーク機器はこれに限定されるものではなく、スイッチ、ハブ、ファイアウォール等が挙げられる。

また、ネットワーク機器やコンピュータを互いに通信可能にするための接続は、有線であっても無線であっても良い。

【００１８】
サーバ３は、管理対象ネットワーク２に接続される端末５の使用を管理するためのコンピュータであり、ルータ４等のネットワーク機器を介して管理対象ネットワーク２と接続される。サーバ３は、管理対象ネットワーク２に対して、端末５の使用を許可することを示す端末使用許可情報を所定の送信間隔時間ごとに同報送信するものである。
端末５は、企業等の管理主体に属するユーザが使用するコンピュータであり、ルータ４等のネットワーク機器を介して管理対象ネットワーク２と接続される。端末５は、サーバ３から同報送信される情報を受信し、端末使用許可情報を受信した場合には、使用可能状態（ユーザによって使用できる状態）に遷移するものである。すなわち、端末５は、自らを使用可能状態に遷移させる前に、自らが使用可能状態に遷移して良いか否かの判定を行う。
サーバ３と端末５の動作の詳細は後述する。
【００１９】
図２は、サーバ３および端末５を実現するコンピュータのハードウエア構成図である。尚、図２のハードウエア構成は一例であり、用途、目的に応じて様々な構成を採ることが可能である。
コンピュータは、制御部１１、記憶部１２、入力部１３、表示部１４、通信制御部１５等が、バス１９を介して接続される。
【００２０】
制御部１１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等で構成される。
【００２１】
ＣＰＵは、記憶部１２、記録媒体等に格納されるプログラムをＲＡＭ上のワークメモリ領域に呼び出して実行し、バス１９を介して接続された各装置を駆動制御し、コンピュータが行う処理を実現する。
ＲＡＭは、揮発性メモリであり、記憶部１２、記録媒体等からロードしたプログラム、データ等を一時的に保持するとともに、制御部１１が各種処理を行う為に使用するワークエリアを備える。
【００２２】
記憶部１２は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、フラッシュメモリ、ＨＤＤ（ハードディスクドライブ）等であり、制御部１１が実行するプログラム、プログラム実行に必要なデータ等が格納される。プログラムに関しては、ＢＩＯＳ（Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　Ｓｙｓｔｅｍ）、ブートローダ、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）に相当する制御プログラムや、後述する処理をコンピュータに実行させるためのアプリケーションプログラムが格納されている。
これらの各プログラムコードは、制御部１１により必要に応じて読み出されてＲＡＭに移され、ＣＰＵに読み出されて各種の手段として実行される。
記憶部１２は、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等を介して接続される外部記憶装置（ＵＳＢメモリ、外付型ハードディスク等）であっても良い。
【００２３】
入力部１３は、データの入力を行い、例えば、キーボード、マウス等のポインティングデバイス、テンキー等の入力装置を有する。
入力部１３を介して、コンピュータに対して、操作指示、動作指示、データ入力等を行うことができる。
表示部１４は、ＣＲＴモニタ、液晶パネル等のディスプレイ装置、ディスプレイ装置と連携してコンピュータのビデオ機能を実現するための論理回路等（ビデオアダプタ等）を有する。
通信制御部１５は、通信制御装置、通信ポート等を有し、コンピュータとネットワーク間の通信を媒介する通信インタフェースであり、ネットワークを介して、他のコンピュータ間との通信制御を行う。ネットワークは、有線、無線を問わない。

バス１９は、各装置間の制御信号、データ信号等の授受を媒介する経路である。

【００２４】

図３は、サーバ３の記憶部１２に記憶されるプログラムの一例を示す図である。

サーバ３の記憶部１２には、ＢＩＯＳ３１、ブートローダ３２、ＯＳ３３、使用管理ＡＰ（ＡＰｐｌｉｃａｔｉｏｎ）３４等のプログラムが記憶されている。

ＢＩＯＳ３１は、各種のハードウエアとの入出力を行うためのプログラムである。サーバ３の電源投入時には、ＢＩＯＳ３１が記憶部１２から読み出されて実行される。ＢＩＯＳ３１では、各種のハードウエアの初期化を行い、ブートローダ３２を読み込む。

ブートローダ３２は、ＯＳ３３等の特定のプログラムをロードして起動するためのプログラムである。ブートローダ３２は、ＢＩＯＳ３１によって読み出され、ＯＳ３３等の特定のプログラムをロードする。尚、一般には、記憶部１２のブートセクタ（ブートブロック）に記憶されるプログラムを一次ブートローダと呼び、一次ブートローダに読み込まれてＯＳ３３等の特定のプログラムをロードするプログラムを二次ブートローダと呼ぶ。

ＯＳ３３は、各種のハードウエアを抽象化したインタフェースをアプリケーションプログラムに提供したり、複数のアプリケーションプログラムを同時に利用する際に互いに独立して効率的に処理が行えるように資源を管理したりするなど、コンピュータの基本的な機能を提供する為のプログラムである。

【００２５】

使用管理ＡＰ３４は、管理対象ネットワーク２に接続される端末５（コンピュータ）の使用を管理するためのプログラムである。サーバ３は、ＯＳ３３が起動された後、使用管理ＡＰ３４を実行し、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信する。

具体的には、サーバ３は、例えば、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）レベルのブロードキャスト通信を行う。ＩＰレベルのブロードキャスト通信では、送信先アドレスを「ブロードキャストアドレス」と呼ばれる特別なアドレスに設定して、端末使用許可情報のパケットを送信する。

端末使用許可情報は、特に限定しないが、例えば、ワンタイムパスワードのように、時間帯によって異なる内容とすることが望ましい。また、端末使用許可情報は、例えば、暗号化して送信し、正規の端末５によってのみ復号できるものとしても良い。

【００２６】

ブロードキャストアドレスには、例えば、リミテッドブロードキャストアドレス、またはディレクティッドブロードキャストアドレスと呼ばれるものを指定することができる。

リミテッドブロードキャストアドレスとは、全てのビットが１となっているＩＰアドレスのことである。例えば、ＩＰｖ４（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｖｅｒｓｉｏｎ　４）であれば、「２５５．２５５．２５５．２５５」がリミテッドブロードキャストアドレスとなる。リミテッドブロードキャストアドレスを指定してブロードキャスト通信を行うと、送信元が接続されているネットワークセグメント（イーサネット（登録商標）であればコリジョンセグメント）内の全てのコンピュータに対してデータが送信される。一方、ルータ４を介して接続されている他のネットワークセグメントへは送信されない。

ディレクティッドブロードキャストアドレスとは、ネットワークアドレス部は変えずに、ホストアドレス部のビットを全て１にしたＩＰアドレスである。例えば、ＩＰｖ４における「１９２．１６８．０」というネットワークアドレスに対しては、ホストアドレス部（下位の８ビット）を全て１にした「１９２．１６８．０．２５５」が、ディレクティッドブロードキャストアドレスとなる。ディレクティッドブロードキャストアドレスを指定してブロードキャスト通信を行うと、特定のネットワークアドレス（前述の例では、「１９２．１６８．０」）を持つ全てのコンピュータに対してデータが送信される。

【００２７】

図１に示すように、管理対象ネットワーク２が、複数のルータ４によって接続されて複数のネットワークセグメントを有している場合を考える。また、管理対象ネットワーク２

は、例えば、「１９２．１６８．０」～「１９２．１６８．９」の１０種類のネットワークアドレスを利用して構築されているものとする。

サーバ３は、１０種類全てのネットワークアドレスに対応するディレクティッドブロードキャストアドレスを指定して、端末使用許可情報のパケットを同時にブロードキャスト通信する。

また、サーバ３をネットワークアドレスごとに配置し、それぞれのサーバ３が、リミテッドブロードキャストアドレスを指定して、端末使用許可情報のパケットをブロードキャスト通信するようにしても良い。この場合、全てのサーバ３を統括する統括サーバ（不図示）を設置し、統括サーバが各サーバ３に対してブロードキャスト通信の実行を指示することで、ブロードキャスト通信の送信タイミングの同期を取ることができる。

【００２８】

図４は、第１の実施の形態における端末５の記憶部１２に記憶されるプログラムの一例を示す図である。

端末５の記憶部１２には、ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３、認証ＡＰ５５および監視ＡＰ５６を含む記憶部暗号化ＡＰ５４等のプログラムが記憶されている。

ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３は、図３に示すＢＩＯＳ３１、ブートローダ３２、ＯＳ３３と同様である。尚、第１の実施の形態では、端末５のブートローダ５２は、記憶部暗号化ＡＰ５４をロードする。

【００２９】

記憶部暗号化ＡＰ５４は、自らの記憶部１２に記憶される情報を自動的に暗号化し、かつ使用可能状態（ユーザによって使用できる状態）では復号して読み取り可能とするためのプログラムである。記憶部暗号化ＡＰ５４は、コンピュータにインストールされて初期設定が行われると、記憶部１２に記憶されている情報を暗号化する。また、記憶部暗号化ＡＰ５４は、インストール後に記憶部１２に記憶される情報も暗号化する。暗号化対象となる情報は、ユーザが明示的に指示して記憶されるデータだけでなく、ＯＳ５３、アプリケーションプログラムなどのプログラム、ＯＳ５３によって利用されるシステムファイル領域、アプリケーションプログラムによって利用される各種データなども含む。但し、ＢＩＯＳ５１、ブートローダ５２、記憶部暗号化ＡＰ５４、記憶部暗号化ＡＰ５４によって利用されるデータについては、暗号化しない。

【００３０】

第１の実施の形態においては、使用可能状態（ユーザによって使用できる状態）への遷移は、予め定められた暗号化解除認証が成功したことを意味する。暗号化解除認証は、記憶部暗号化ＡＰ５４の初期設定時に設定する。

記憶部暗号化ＡＰ５４がインストールされた端末５は、暗号化解除認証が成功すると、自らを使用可能状態に遷移させ、暗号化した情報を復号して読み取り可能とする。

暗号化解除認証が成功しなければＯＳ５３も復号しない為、ユーザはＯＳ５３でさえも起動することができない。

【００３１】

認証ＡＰ５５は、記憶部暗号化ＡＰ５４の一部であって、暗号化解除認証を実行するためのプログラムである。

第１の実施の形態においては、暗号化解除認証とは、ユーザ認証とパケット認証とする。

ユーザ認証とは、ユーザを識別するための識別情報を受け付けて、端末５の使用が許可されているユーザかどうかを認証する。ユーザを識別するための識別情報としては、例えば、暗証番号、パスワード、ユーザに配布されるＩＣカードの情報、ユーザの生体情報（指紋、虹彩、静脈、声紋、顔形など）などが挙げられる。以下では、説明を簡単にする為に、ユーザ認証は、パスワードを識別情報とした認証であるパスワード認証を行うものとする。

パケット認証とは、管理対象ネットワーク２に流れるパケットに基づいて行う認証を意味する。具体的には、パケット認証は、使用管理ＡＰ３４がインストールされたサーバ３

から送信される端末使用許可情報のパケットを受信したかどうかを認証する。
記憶部暗号化ＡＰ５４がインストールされた端末５は、ブートローダ５２によって記憶部暗号化ＡＰ５４がロードされると、認証ＡＰ５５の機能によって、パスワード認証およびパケット認証を実行する。
尚、サーバ３が端末使用許可情報を暗号化して送信する場合、記憶部暗号化ＡＰ５４は、パスワード認証が成功した場合にのみ、端末使用許可情報の復号を可能とするようにしても良い。
【００３２】
監視ＡＰ５５は、記憶部暗号化ＡＰ５４の一部であって、自らを使用不可能状態（ユーザによって使用できない状態）に遷移させるかどうかを監視するためのプログラムである。
第１の実施の形態においては、監視ＡＰ５５は、所定の監視間隔時間ごとに、端末使用許可情報のパケットが直近の所定の監視間隔時間内に受信されたかどうかを確認し、受信されていない場合には、使用不可能状態に自らを遷移させる。
【００３３】
図５は、第１の実施の形態における端末５の起動処理の詳細を示すフローチャートである。図５の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。
【００３４】
端末５の制御部１１は、電源が投入されると、記憶部１２からＢＩＯＳ５１を読み出して起動することで、各種のハードウエアの初期化を行い、ブートローダ５２を読み込む（Ｓ１０１）。
次に、制御部１１は、ブートローダ５２を実行することで、記憶部暗号化ＡＰ５４を読み出し、記憶部暗号化ＡＰ５４の一部である認証ＡＰ５５の機能によって、パスワード認証を行う（Ｓ１０２）。Ｓ１０２では、制御部１１は、表示部１４にパスワード入力画面を表示する。これに対して、ユーザは、入力部１３を介してパスワードを入力する。制御部１１は、入力されたパスワードを認証し、認証が成功すると、Ｓ１０３に進む。一方、認証が失敗すると、制御部１１は、処理を終了し、シャットダウン等を行う。
尚、シャットダウンは、使用不可能状態（ユーザによって使用できない状態）に自らを遷移させる処理の一例に過ぎず、例えば、再起動、ＯＳ５３からのログオフなど、その他の処理を行っても良い。また、以下の説明においても同様とする。
【００３５】
次に、制御部１１は、認証ＡＰ５５の機能によって、パケット認証を行う（Ｓ１０３）。Ｓ１０３では、制御部１１は、通信制御部１５を介して、同報送信されている情報を監視する。サーバ３からの端末使用許可情報が受信されたことを確認すると、制御部１１は、パケット認証が成功したものとして、Ｓ１０４に進む。一方、所定のタイムアウト時間（少なくとも、サーバ３による端末使用許可情報の送信間隔時間よりも長い時間）を経過してもサーバ３からの端末使用許可情報が受信されない場合、パケット認証が失敗したものとして、処理を終了し、シャットダウン等を行う。
尚、Ｓ１０２とＳ１０３は、いずれを先に実行しても良い。
【００３６】
次に、制御部１１は、記憶部暗号化ＡＰ５４の機能によって、記憶部１２を復号して読み取り可能とし、ＯＳ５３を読み出して起動する（Ｓ１０４）。以降の処理はＯＳ５３の機能によって実行され、ユーザは端末５を使用することが可能となる。
【００３７】
図６は、第１の実施の形態における端末５の監視処理の詳細を示すフローチャートである。図６の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。
【００３８】
端末５の制御部１１は、記憶部暗号化ＡＰ５４の一部である監視ＡＰ５６の機能によっ

て、パケット監視を行う（Ｓ２０１）。Ｓ２０１では、制御部１１は、通信制御部１５を介して、同報送信されているパケットを監視し、サーバ３からの端末使用許可情報のパケットを受信すると、パケット受信フラグをＲＡＭまたは記憶部１２に記憶しておく。所定の監視間隔時間（少なくとも、サーバ３による端末使用許可情報の送信間隔時間よりも長い時間）が経過すると、制御部１１は、Ｓ２０２に進む。

次に、制御部１１は、端末使用許可情報のパケットが直近の監視間隔時間内に受信されたか、すなわちパケット受信フラグがＲＡＭまたは記憶部１２に記憶されているかどうかを確認する（Ｓ２０２）。

パケット受信フラグが記憶されている場合（Ｓ２０２のＹｅｓ）、制御部１１は、パケット受信フラグを削除し、Ｓ２０１に進む。

パケット受信フラグが記憶されていない場合（Ｓ２０２のＮｏ）、制御部１１は、処理を終了し、シャットダウン等を行う。

【００３９】

以上、第１の実施の形態では、サーバ３は、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信し、端末５は、端末使用許可情報を受信すると、自らを使用可能状態に遷移させる。これによって、管理対象ネットワーク２に接続していない状態で端末５の使用を試みても、端末５を使用することはできない。従って、管理主体の施設外での不正使用を防止することができる。第１の実施の形態における使用管理システム１は、サーバ３および端末５として通常のコンピュータを用いれば良いので、数多くのコンピュータを管理する場合もコストをかけず、確実に使用を管理することができる。

【００４０】

また、端末５は、定期的に端末使用許可情報のパケットが受信されたかどうか確認し、受信されていない場合、自らを使用不可能状態に遷移させる。これによって、使用可能状態で端末５を管理主体の施設外に持ち運ばれても、端末５をそのまま使用することを防止することができる。また、使用可能状態では、端末５は管理対象ネットワーク２に接続されていることになるので、ユーザがセキュリティポリシーを守っているか否かをリアルタイムで監視することもできる。

【００４１】

更に、認証ＡＰ５５が行うパケット認証は、記憶部暗号化ＡＰ５４における暗号化解除認証となっているので、パケット認証が成功しなければ、端末５の記憶部１２に記憶されている情報は暗号化されたままである。従って、仮に記憶部１２であるハードディスクを取り外して、ハードディスクの解析を試みても、情報を読み取ることはできない。

【００４２】

尚、前述の説明では、認証ＡＰ５５がパスワード認証およびパケット認証を行うものとしたが、認証ＡＰ５５はパケット認証のみを行うようにして、ＯＳ５３の機能によってパスワード認証を行うようにしても良い。

また、前述の説明では、認証ＡＰ５５および監視ＡＰ５６が記憶部暗号化ＡＰ５４の一部としたが、これらは別のプログラムとして実行されても良い。

【００４３】

＜第２の実施の形態＞

第２の実施の形態は、第１の実施形態と比較して、端末５にインストールされるプログラムが異なる。以下、第１の実施の形態と同じ要素には同じ番号を付し、重複する説明を省略する。

【００４４】

図７は、第２の実施の形態における端末５の記憶部１２に記憶されるプログラムの一例を示す図である。

端末５の記憶部１２には、ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３、認証ＡＰ５５および監視ＡＰ５６を含む検疫ＡＰ５７等のプログラムが記憶されている。

第２の実施の形態では、端末５のブートローダ５２は、ＯＳ５３をロードする。そして

、ＯＳ５３が起動された後、検疫ＡＰ５７がロードされ、検疫ＡＰ５７の一部である認証ＡＰ５５、監視ＡＰ５６が実行される。
第２の実施の形態においては、使用可能状態（ユーザによって使用できる状態）への遷移は、検疫ＡＰ５７の一部である認証ＡＰ５５による認証が成功したことを意味する。
尚、認証ＡＰ５５はパケット認証のみを行うようにして、ＯＳ５３の機能によってパスワード認証を行うようにしても良い。
【００４５】
検疫ＡＰ５７は、端末５の各種情報を収集し、セキュリティポリシーに適合しているかどうかを検疫するためのプログラムである。収集する情報は、例えば、ウィルス対策ソフトのパターンファイルのバージョン、ＯＳ５３のバージョン、その他セキュリティポリシーに応じて必要な情報である。
また、その他には、認証ＡＰ５５によって行われる認証の結果、および監視ＡＰ５６によって行われる監視の結果が、実行時刻とともに収集される。
収集した情報は、検疫ＡＰ５７の機能によって、定期的にサーバ３に送信され、管理者が確認できる。
【００４６】
第２の実施の形態では、検疫ＡＰ５７の機能によって、認証ＡＰ５５による認証の結果および監視ＡＰ５６による監視の結果が収集されるので、万が一不正使用が行われた場合であっても、不正使用後に端末５が管理対象ネットワーク２に接続されることで、不正使用の履歴を追跡することができる。
【００４７】
＜第３の実施の形態＞
第３の実施の形態は、第１の実施形態と比較して、端末５のハードウエア構成、端末５にインストールされるプログラムが異なる。以下、第１の実施の形態と同じ要素には同じ番号を付し、重複する説明を省略する。
【００４８】
図８は、第３の実施の形態における使用管理システム１ａの全体構成図である。
使用管理システム１ａは、管理対象ネットワーク２に接続されるサーバ３、端末５ａの他に、電波発信装置６、発光装置７等を構成に含む。
電波発信装置６は、端末５ａの使用を許可することを示す特定の周波数を有する電波、または端末５ａの使用を許可することを示す情報を搬送する電波を発信するものである。電波発信装置６は、管理主体の施設外では受信できないように、管理主体の施設に応じて適切な強度、指向性を有する電波を発信する。
発光装置７は、端末５ａの使用を許可することを示す特定の波長を有する光、または端末５ａの使用を許可することを示す情報を搬送する光を発光するものである。
【００４９】
図９は、第３の実施の形態における端末５ａを実現するコンピュータのハードウエア構成図である。尚、図９のハードウエア構成は一例であり、用途、目的に応じて様々な構成を採ることが可能である。
コンピュータは、制御部１１、記憶部１２、入力部１３、表示部１４、通信制御部１５、電波受信部１６、受光部１７、ＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）受信部１８等が、バス１９を介して接続される。
【００５０】
電波受信部１６は、電波発信装置６から発信される電波を受信する。電気受信部１６は、制御部１１からの要求に応じて、端末５ａの使用を許可することを示す電波を受信したかどうかを応答する。
受光部１７は、発光装置７から発光される光を受信する。受光部１７は、制御部１１からの要求に応じて、端末５ａの使用を許可することを示す光を受光したかどうかを応答する。
ＧＰＳ受信部１８は、ＧＰＳ衛星からの信号を受信し、端末５ａの現在位置を特定する

。ＧＰＳ受信部１８は、制御部１１からの要求に応じて、端末５ａの現在位置（緯度、経度）を応答する。

【００５１】

図１０は、第３の実施の形態における端末５ａの記憶部１２に記憶されるプログラムの一例を示す図である。

端末５ａの記憶部１２には、ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３、認証ＡＰ５５ａおよび監視ＡＰ５６ａを含む記憶部暗号化ＡＰ５４ａ等のプログラムが記憶されている。

ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３は、第１の実施の形態、第２の実施の形態と同様である。尚、第３の実施の形態では、端末５ａのブートローダ５２は、記憶部暗号化ＡＰ５４ａをロードする。

また、記憶部暗号化ＡＰ５４ａも、認証ＡＰ５５ａおよび監視ＡＰ５６ａを除いては、第１の実施の形態と同様である。

【００５２】

認証ＡＰ５５ａは、記憶部暗号化ＡＰ５４ａの一部であって、暗号化解除認証を実行するためのプログラムである。

第３の実施の形態においては、暗号化解除認証とは、パスワード認証（ユーザ認証）、パケット認証、ＧＰＳ認証、電波認証、光認証とする。

パスワード認証およびパケット認証は、第１の実施の形態と同様である。

ＧＰＳ認証とは、ＧＰＳ受信部１８によって受信される位置情報が端末５ａの使用を許可する端末使用許可範囲内かどうかの認証である。端末使用許可範囲は、記憶部暗号化ＡＰ５４ａの初期設定時に設定する。

電波認証とは、電波受信部１６によって受信される電波が端末５ａの使用を許可するものかどうかの認証である。端末５ａの使用を許可することを示す電波の定義は、記憶部暗号化ＡＰ５４ａの初期設定時に設定する。

光認証とは、受光部１７によって受光される光が端末５ａの使用を許可するものかどうかの認証である。端末５ａの使用を許可することを示す光の定義は、記憶部暗号化ＡＰ５４ａの初期設定時に設定する。

記憶部暗号化ＡＰ５４ａがインストールされた端末５ａは、ブートローダ５２によって記憶部暗号化ＡＰ５４ａがロードされると、認証ＡＰ５５ａの機能によって、パスワード認証、パケット認証、ＧＰＳ認証、電波認証、光認証を実行する。

【００５３】

監視ＡＰ５５ａは、記憶部暗号化ＡＰ５４ａの一部であって、自らを使用不可能状態（ユーザによって使用できない状態）に遷移させるかどうかを監視するためのプログラムである。

第３の実施の形態においては、監視ＡＰ５５ａは、パケット監視、ＧＰＳ監視、電波監視、光監視を行う。

パケット監視とは、第１の実施の形態と同様の監視内容であって、所定の監視間隔時間ごとに、端末使用許可情報のパケットが直近の所定の監視間隔時間内に受信されたかどうかの監視である。

ＧＰＳ監視とは、所定の監視間隔時間ごとに、ＧＰＳ受信部１８によって受信される位置情報が端末５ａの使用を許可する端末使用許可範囲内かどうかの監視である。

電波監視とは、所定の監視間隔時間ごとに、端末５ａの使用を許可する電波が直近の所定の監視間隔時間内に受信されたかどうかの監視である。

光監視とは、所定の監視間隔時間ごとに、端末５ａの使用を許可する光が直近の所定の監視間隔時間内に受信されたかどうかの監視である。

【００５４】

図１１は、セキュリティレベル表６１の一例を示す図である。

第３の実施の形態では、端末５ａごとに異なるセキュリティレベルを設定する。セキュリティレベルは、記憶部暗号化ＡＰ５４ａの初期設定時に設定する。図１１に示すセキュ

リティレベル表６１は、認証ＡＰ５５ａによる認証、および監視ＡＰ５６ａによる監視の両方に対して適用される。但し、監視ＡＰ５６ａによる監視については、ユーザが煩わしくないように、パスワードによる監視を行わなくても良い。

例えば、図１１に示す例では、レベル１の端末５ａに対する認証は、パスワード認証のみを行う。一方、レベル５の端末５ａに対する認証は、パスワード認証、パケット認証、ＧＰＳ認証、電波認証、光認証の全てを行う。

【００５５】

尚、セキュリティレベル表６１は、図１１に示す例に限定されるものではない。図１１に示すレベル３に代わる例としては、例えば、パスワード認証、およびパケット認証（監視）を必須とし、更に、ＧＰＳ認証（監視）、電波認証（監視）、光認証（監視）のいずれか１つの認証が成功すればセキュリティレベル表６１を満たすとしても良い。

また、図１１に示すレベル４に代わる例としては、例えば、パスワード認証、およびパケット認証（監視）を必須とし、更に、ＧＰＳ認証（監視）、電波認証（監視）、光認証（監視）のいずれか２つの認証が成功すればセキュリティレベル表６１を満たすとしても良い。

【００５６】

図１２は、第３の実施の形態における端末５ａの起動処理の詳細を示すフローチャートである。図１２の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末５ａの使用を許可することを示す端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

【００５７】

Ｓ３０１～Ｓ３０３は、第１の実施の形態における図５のＳ１０１～Ｓ１０３と同様である。

Ｓ３０３が終了すると、端末５ａの制御部１１は、認証ＡＰ５５ａの機能によって、ＧＰＳ認証（Ｓ３０４）、電波認証（Ｓ３０５）、光認証（Ｓ３０６）を行う。

次に、制御部１１は、自らに設定されたセキュリティレベルに対応するセキュリティレベル表６１を満たしているかどうか、すなわちセキュリティレベルに応じた認証が全て成功しているかどうかを確認する（Ｓ３０７）。

成功している場合（Ｓ３０７のＹｅｓ）、制御部１１は、記憶部暗号化ＡＰ５４ａの機能によって、記憶部１２を復号して読み取り可能とし、ＯＳ５３を読み出して起動する（Ｓ３０８）。以降の処理はＯＳ５３の機能によって実行され、ユーザは端末５ａを使用することが可能となる。

成功していない場合（Ｓ３０７のＮｏ）、制御部１１は、処理を終了し、シャットダウン等を行う。

尚、Ｓ３０２～Ｓ３０６は、どのような順番で実行しても良い。

【００５８】

図１３は、第３の実施の形態における端末５ａの監視処理の詳細を示すフローチャートである。図１３の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

【００５９】

端末５ａの制御部１１は、監視ＡＰ５６ａの機能によって、パケット監視（Ｓ４０１）、ＧＰＳ監視（Ｓ４０２）、電波監視（Ｓ４０３）、光監視（Ｓ４０４）を行う。

制御部１１は、パケット監視において、サーバ３からの端末使用許可情報のパケットを受信すると、パケット受信フラグをＲＡＭまたは記憶部１２に記憶しておく。また、制御部１１は、ＧＰＳ監視において、ＧＰＳ受信部１８によって受信される位置情報をＲＡＭまたは記憶部１２に記憶しておく。また、制御部１１は、電波監視において、端末５ａの使用を許可することを示す電波を受信すると、電波受信フラグをＲＡＭまたは記憶部１２に記憶しておく。また、制御部１１は、光監視において、端末５ａの使用を許可することを示す光を受光すると、光受光フラグをＲＡＭまたは記憶部１２に記憶しておく。

所定の監視間隔時間（少なくとも、サーバ３による端末使用許可情報の送信間隔時間よ

りも長い時間）が経過すると、制御部１１は、Ｓ４０５に進む。
【００６０】
次に、制御部１１は、自らに設定されたセキュリティレベルに対応するセキュリティレベル表６１を満たしているかどうか、すなわちセキュリティレベルに応じた監視が全て成功しているかどうかを確認する（Ｓ４０５）。
成功している場合（Ｓ４０５のＹｅｓ）、制御部１１は、パケット受信フラグ、位置情報、電波受信フラグ、光受光フラグを削除し、Ｓ４０１に進む。
成功していない場合（Ｓ４０５のＮｏ）、制御部１１は、処理を終了し、シャットダウン等を行う。
尚、Ｓ４０１～Ｓ４０４は、どのような順番で実行しても良い。
【００６１】
以上、第３の実施の形態では、サーバ３は、パスワード認証、パケット認証に加えて、ＧＰＳ認証、電波認証、光認証も行う。これによって、端末５ａのハードウエア構成や使用する環境に適した認証を行うことができ、利便性を高めることができる。
特に、様々な認証の仕組みを備えることで、端末５ａごとにセキュリティレベルを設定し、セキュリティレベルに適した認証を行うことができる。
例えば、シンクライアント端末のように、記憶部１２を具備しないパソコンの場合、盗難や紛失などが発生しても、漏洩する情報自体が存在しない為、セキュリティレベルを低く設定し、利便性を高めることができる。一方、重要情報を記憶部１２に記憶して使用する端末については、セキュリティレベルを高く設定し、確実に使用を管理することができる。
【００６２】
尚、前述の説明では、端末５ａには、記憶部暗号化ＡＰ５４ａがインストールされるものとしたが、第２の実施の形態における検疫ＡＰ５７と同等のプログラムをインストールしても良い。この場合、認証ＡＰ５５ａによって行われる認証の結果、および監視ＡＰ５６ａによって行われる監視の結果が、実行時刻とともに収集され、定期的にサーバ３に送信される。
【００６３】
＜第４の実施の形態＞
第４の実施の形態は、第３の実施形態と比較して、端末５ｂにインストールされるプログラムが異なる。また、図１１に示すセキュリティ表６１に代えて、図１５に示す安全指数表２１、および図１６に示すレベル別起動設定２２を記憶部１２に記憶している。以下、第１、第３の実施の形態と同じ要素には同じ番号を付し、重複する説明を省略する。
【００６４】
図１４は、端末５ｂにインストールされるプログラムの一例を示す図、図１５は、安全指数表２１の一例を示す図、図１６は、レベル別起動設定２２の一例を示す図である。
図１４に示すように、端末５ｂの記憶部１２には、ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３、認証ＡＰ５５ｂおよび監視ＡＰ５６ｂを含む記憶部暗号化ＡＰ５４ｂ等のプログラムが記憶されている。
ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３は、第１～第３の実施の形態と同様である。尚、第４の実施の形態では、端末５ｂのブートローダ５２は、記憶部暗号化ＡＰ５４ｂをロードする。
また、記憶部暗号化ＡＰ５４ｂも、認証ＡＰ５５ｂおよび監視ＡＰ５６ｂを除いては、第１の実施の形態と同様である。
【００６５】
認証ＡＰ５５ｂは、記憶部暗号化ＡＰ５４ｂの一部であって、暗号化解除認証を実行するためのプログラムである。
第４の実施の形態では、暗号化解除認証として、少なくともパケット認証を含む複数種類の認証処理を実行する。例えば、第３の実施の形態と同様に、パスワード認証（ユーザ認証）、パケット認証、ＧＰＳ認証、電波認証、および光認証とする。

また、認証処理ごとに安全性の度合いを示す安全指数が図１５の安全指数表２１に示すように予め定められている。端末５ｂは、各認証処理の結果と、安全指数とに基づいて自らのセキュリティレベルを算出し、セキュリティレベルに応じて使用できる機能を制限して起動する。例えば、図１６のレベル別起動設定２２に示すように、セキュリティレベルが「低」であると判定した場合は、ユーザが使用できない状態である使用不可状態とする。また、セキュリティレベルが「中」であると判定した場合は、使用できる機能を制限して起動する機能制限状態に遷移させる。また、セキュリティレベルが「高」であると判定した場合は、制限を設けずに使用可能とする使用可能状態に遷移させる。

各種認証処理およびセキュリティレベルの算出、判定は、記憶部暗号化ＡＰ５４ｂの認証ＡＰ５５ｂによる認証、および監視ＡＰ５６ｂによる監視の両方に対して適用される。但し、監視ＡＰ５６ｂによる監視については、ユーザが煩わしくないように、パスワードによる監視を行わなくても良い。

【００６６】

図１７は、第４の実施の形態における端末５ｂの起動処理の詳細を示すフローチャートである。第４の実施の形態における端末５ｂの起動処理では、図１７の例では、パスワード認証、パケット認証、ＧＰＳ認証、電波認証、および光認証を行う。図１７の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末５ｂの使用を許可することを示す端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

尚、安全指数表２１やレベル別起動設定２２は、図１５、図１６に示す例に限定されるものではない。図１６のレベル別起動設定２２では、セキュリティレベルを「低」、「中」、「高」の３レベルに分類した例を示しているが、「低」および「高」の２レベル、または４レベル以上の分類としてもよい。また、機能制限状態としては、例えば、「メディアへの書き出し不可」や「記憶部の所定記憶領域へのアクセス不可」、「メール送信不可」等が挙げられる。

【００６７】

Ｓ５０１～Ｓ５０６は、第３の実施の形態における図１２のＳ３０１～Ｓ３０６と同様である。すなわち、端末５ｂの制御部１１は、ＢＩＯＳ起動、パスワード認証、パケット認証、ＧＰＳ認証、電波認証、光認証を行う。ここで、各認証処理における認証の結果は、パケット受信フラグ、位置情報、電波受信フラグ、光受光フラグ等としてＲＡＭまたは記憶部１２に記憶しておく。認証成功の場合は、該当するフラグを「１」にセットし、認証失敗の場合は該当するフラグを「０」にセットする。

Ｓ５０６が終了すると、端末５ｂの制御部１１は、認証ＡＰ５５ｂの機能によって、安全指数表２１に設定されている各認証処理の安全指数を認証処理結果を示す各フラグの値（「１」または「０」）に乗じ、安全指数の合計値を求める（Ｓ５０７）。

制御部１１は、安全指数の合計値からセキュリティレベルを判定し（Ｓ５０８）、「高」レベルであれば（Ｓ５０８の「高」）、記憶部暗号化ＡＰ５４ｂの機能によって、記憶部１２を復号して読み取り可能とし、ＯＳ５３を読み出して起動する（Ｓ５０９）。以降の処理はＯＳ５３の機能によって実行され、ユーザは端末５ｂを制限なく使用することが可能となる。

一方、安全指数の合計値が「中」レベルであれば（Ｓ５０８の「中」）、制御部１１は、「中」レベルに該当する状態である機能制限状態に端末５ｂを遷移させる。例えば、メディアへの書き出し機能を制限する場合は、記憶部暗号化ＡＰ５４ｂの機能によって、記憶部１２を復号して読み取り可能とし、ＯＳ５３を読み出して以降の処理はＯＳ５３の機能によって実行されるが、メディアへの書き出し機能は使用不可とされる（Ｓ５１０）。

また、安全指数の合計値が「低」レベルであれば（Ｓ５０８の「低」）、制御部１１は、「低」レベルに該当する状態である使用不可状態に端末５ｂを遷移させる。すなわち、処理を終了し、シャットダウン等を行う。

尚、Ｓ５０２～Ｓ５０６は、どのような順番で実行しても良い。

【００６８】

例えば、図１８に示すようにパスワード認証、パケット認証、電波認証、光認証が認証成功し、ＧＰＳ認証は認証失敗した場合は、安全指数の合計値は「２４」となる。この場合、図１６に示すレベル別起動設定２２に従って、セキュリティレベルは「高」レベルと判定されるため、端末５ｂは全機能を使用可能として、起動される。

【００６９】

図１９は、第４の実施の形態における端末５ｂの監視処理の詳細を示すフローチャートである。図１９の処理を行う前提として、サーバ３は、管理対象ネットワーク２に対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

【００７０】

Ｓ６０１～Ｓ６０４において、端末５ｂの制御部１１は、監視ＡＰ５６ｂの機能によって、第３の実施の形態における図１３のＳ４０１～Ｓ４０４と同様に、パケット監視、ＧＰＳ監視、電波監視、光監視を行う。監視処理においても、制御部１１は各監視処理の結果に応じて該当するフラグを「１」または「０」に更新し、ＲＡＭまたは記憶部１２に記憶しておく。

所定の監視間隔時間（少なくとも、サーバ３による端末使用許可情報の送信間隔時間よりも長い時間）が経過すると、制御部１１は、Ｓ６０５に進む。

端末５ｂの制御部１１は、監視ＡＰ５６ｂの機能によって、安全指数表２１に設定されている安全指数を対応する監視処理の結果を示す各フラグの値（「１」または「０」）に乗じ、安全指数の合計値を求める（Ｓ６０５）。

制御部１１は、安全指数の合計値からセキュリティレベルが前回の監視処理時と比較して低下したか否かを判定し（Ｓ６０６）、同じセキュリティレベルを維持している場合（Ｓ６０６のＮｏ）は、制御部１１はＳ６０１に進む。

セキュリティレベルが低下した場合であっても（Ｓ６０６のＹｅｓ）、レベルが「低」でない場合は（Ｓ６０７のＮｏ）、制御部１１は、該当する機能制限状態に端末５ｂを遷移させる（Ｓ６０８）。

セキュリティレベルが低下し（Ｓ６０６のＹｅｓ）、「低」となった場合は（Ｓ６０７のＹｅｓ）、制御部１１は、「低」レベルに該当する状態である使用不可状態に端末５ｂを遷移させる。すなわち、処理を終了し、シャットダウン等を行う。

尚、Ｓ６０１～Ｓ６０４は、どのような順番で実行しても良い。

【００７１】

以上、第４の実施の形態では、サーバ３は、少なくともパケット認証を含む複数種類の認証処理を実行し、その認証結果によって安全指数の合計値を求め、これによってセキュリティレベルを判定し、レベルに応じた機能制限を行う。そのため柔軟な認証ポリシ管理を行え、利便性を高めることができる。

特に、様々な認証の仕組みを備えることで、より細かくセキュリティレベルを設定したり、機能制限を行うことも可能となる。

例えば、社内では全ての機能を制限なく使用できるが、端末５ｂを家庭に持ち帰って使用する場合には、使用できる機能を制限することもできる。また、社員等の正当なユーザに認証用の電波発信装置６や発光装置７を持たせれば、通信設備がない状況下であったり、不具合により通信断が生じてパケット認証ができない状況でも、パスワード認証、電波認証、および光認証等の各種の認証処理を組み合わせれば所定機能の使用を可能とすることも可能となる。このように、様々な使用環境に柔軟に対応できる。

【００７２】

尚、前述の説明では、端末５ｂには、記憶部暗号化ＡＰ５４ｂがインストールされるものとしたが、第２の実施の形態における検疫ＡＰ５７と同等のプログラムをインストールしても良い。この場合、認証ＡＰ５５ｂによって行われる認証の結果、および監視ＡＰ５６ｂによって行われる監視の結果が、実行時刻とともに収集され、定期的にサーバ３に送信される。

【００７３】

＜第５の実施の形態＞

第５の実施の形態は、第４の実施の形態と比較して、使用管理システム１の管理対象ネットワーク２の構成、端末５ｂのハードウエア構成、端末５ｂにインストールされるプログラムが異なる。以下、第４の実施の形態と同じ要素には同じ番号を付し、重複する説明を省略する。

【００７４】

図２０は、第５の実施の形態における使用管理システム１ｃの全体構成図である。

使用管理システム１ｃでは、管理対象ネットワーク２として、第１の実施の形態のように閉じた管理対象ネットワーク２ａに加え、公衆の通信ネットワーク２ｃを利用するものも含む。

すなわち、管理対象ネットワーク２ｃは、インターネット、無線通信網、電話回線、携帯電話通信網等を含む公衆のネットワーク（以下、単にインターネット１１という）、インターネットサービスプロバイダ（ＩＳＰ）１２、無線基地局１３等を備える。

また、仮想プライベートネットワーク（ＶＰＮ）として使用管理システム１ｃを構築する場合には、ＶＰＮサーバ１４が設けられる。

【００７５】

ＶＰＮサーバ１４は、サーバ３および端末５ｃのＶＰＮ接続を媒介するサーバであり、暗号化処理や認証処理を行う。端末５ｃからサーバ３へデータを送信する際は、端末５ｃが備えるＶＰＮクライアントＡＰの機能により、データを暗号化してインターネット１１経由でＶＰＮサーバ１４へ伝送する。ＶＰＮサーバ１４は受信した暗号化データを復号してサーバ３へ送信する。

ＩＳＰ１２は、ＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）サーバ等を備え、端末５ｃからのアクセスがあると、その端末５ｃに動的なＩＰアドレスを割り当てる。すなわち、端末５ｃは、認証ＡＰ５５ｃの機能によって起動処理を行う際に、ＩＳＰ１２に対してＩＰアドレスの割り当てをリクエストする。ＩＳＰ１２は管理しているＩＰアドレスの中から利用可能なＩＰアドレスを割り当て、ネットワーク接続時に必要な情報や、認証に必要な情報（例えば、通信事業者情報やＩＳＰ１２の位置情報等）を要求元の端末５ｃに返す。

【００７６】

図２１は、第５の実施の形態における端末５ｃを実現するコンピュータのハードウエア構成図である。尚、図２１のハードウエア構成は一例であり、用途、目的に応じて様々な構成を採ることが可能である。

コンピュータは、制御部１１、記憶部１２、入力部１３、表示部１４、通信制御部１５、電波受信部１６、受光部１７、ＧＰＳ受信部１８、無線通信部２０等が、バス１９を介して接続される。

【００７７】

端末５ｃの無線通信部２０は、公衆の無線ネットワークにアクセスするための通信インタフェースである。公衆無線ネットワークには、無線基地局１３、携帯電話回線、無線ＬＡＮ等が含まれる。

【００７８】

図２２は、第５の実施の形態における端末５ｃの記憶部１２に記憶されるプログラムの一例を示す図である。

端末５ｃの記憶部１２には、ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３、認証ＡＰ５５ｃおよび監視ＡＰ５６ｃを含む記憶部暗号化ＡＰ５４ｃ等のプログラムが記憶されている。

ＢＩＯＳ５１、ブートローダ５２、ＯＳ５３は、第１の実施の形態の実施の形態と同様である。尚、第５の実施の形態では、端末５ｃのブートローダ５２は、記憶部暗号化ＡＰ５４ｃをロードする。

また、記憶部暗号化ＡＰ５４ｃも、認証ＡＰ５５ｃおよび監視ＡＰ５６ｃを除いては、第１の実施の形態と同様である。

【００７９】

認証ＡＰ５５ｃは、記憶部暗号化ＡＰ５４ｃの一部であって、暗号化解除認証を実行するためのプログラムである。

第５の実施の形態では、暗号化解除認証として、パスワード認証（ユーザ認証）、パケット認証、ＧＰＳ認証、電波認証、光認証に加え、ＩＰアドレス認証、無線基地局認証を行うものとする。パスワード認証、パケット認証、ＧＰＳ認証、電波認証、および光認証は、第１、第３の実施の形態と同様である。

【００８０】

ＩＰアドレス認証とは、ＩＳＰ１２から動的に割り当てられるＩＰアドレスに応じて端末５ｃが使用可能かどうかを判断する認証である。例えば、ＩＳＰ１２がＩＰアドレスとともに位置情報を提供する場合、端末５ｃはその位置情報から端末使用許可範囲内かどうかを判断する。端末使用許可範囲は、記憶部暗号化ＡＰ５４ｃの初期設定時に設定する。

【００８１】

無線基地局認証とは、無線基地局１３から受け取った通信事業者情報や各無線基地局１３を識別する基地局識別情報に基づいて端末５ｃが使用許可範囲内にあるかどうかを判断する認証である。端末使用許可範囲は、記憶部暗号化ＡＰ５４ｃの初期設定時に設定する。

端末使用許可範囲としては、例えば、国内であれば使用可とし、国外では使用不可とする。これによって、端末５ｃが盗まれて国外に持ち出された場合には認証失敗となる。

また、無線基地局１３からその無線基地局１３の識別情報（基地局識別情報）を取得できる場合は、取得した基地局識別情報が予め登録した無線基地局１３のものであれば認証成功とし、その他の場合は認証失敗としてもよい。例えば、各無線基地局１３の位置情報が公開されていれば、基地局識別情報に基づいて基地局の位置情報を取得でき、更には端末５ｃの位置を把握できるため、無線基地局単位に、より細かく端末使用許可範囲を設定できるようになる。

更に、通信事業者が、上述の「パケット認証」のように、端末５ｃの使用許可を示すキーパケットを特定の無線基地局１３から間欠的に同報送信するサービスを提供すれば、端末５ｃがキーパケットを受信できる範囲内であれば認証成功とし、そうでなければ認証失敗としてもよい。

【００８２】

記憶部暗号化ＡＰ５４ｃがインストールされた端末５ｃは、ブートローダ５２によって記憶部暗号化ＡＰ５４ｃがロードされると、認証ＡＰ５５ｃの機能によって、パスワード認証、パケット認証、ＩＰアドレス認証、無線基地局認証、ＧＰＳ認証、電波認証、光認証を実行する。

【００８３】

監視ＡＰ５５ｃは、記憶部暗号化ＡＰ５４ｃの一部であって、自らを使用不可能状態（ユーザによって使用できない状態）または機能制限状態（機能の一部が制限された使用可能状態）に遷移させるかどうかを監視するためのプログラムである。

第５の実施の形態においては、監視ＡＰ５５ｃは、パケット監視、ＩＰアドレス監視、無線基地局監視、ＧＰＳ監視、電波監視、光監視を行う。パケット監視、ＧＰＳ監視、電波監視、光監視は、第１、第３の実施の形態と同様の監視内容である。

ＩＰアドレス監視とは、所定の監視間隔時間ごとに、端末５ｃに割り当てられている動的ＩＰアドレスに基づいて端末５ｃが端末使用許可範囲内にあるかどうかの監視である。

無線基地局認証とは、所定の監視間隔時間ごとに、端末５ｃがアクセスした無線基地局１３から受け取った通信事業者情報または各無線基地局１３を識別する基地局識別情報に基づいて端末５ｃが端末使用許可範囲内にあるかどうかの監視である。

【００８４】

図２３は、第５の実施の形態で適用される安全指数表２５の一例である。

図２３の安全指数表２５は図１５に示す第４の実施の形態の安全指数表２１に加え、ＩＰアドレス認証および無線基地局認証についての安全指数が設定されている。また、図２３に示す安全指数表２５は、認証ＡＰ５５ｃによる認証、および監視ＡＰ５６ｃによる監

視の両方に対して適用される。但し、監視ＡＰ５６ｃによる監視については、ユーザが煩わしくないように、パスワードによる監視を行わなくても良い。

【００８５】

図２４は、第５の実施の形態における端末５ｃの起動処理の詳細を示すフローチャートである。図２４の処理を行う前提として、サーバ３は、管理対象ネットワーク２ａ、２ｂに対して、端末５ｃの使用を許可することを示す端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

【００８６】

Ｓ７０１～Ｓ７０３は、第１の実施の形態における図５のＳ１０１～Ｓ１０３と同様である。

Ｓ７０３が終了すると、端末５ｃの制御部１１は、認証ＡＰ５５ｃの機能によって、ＩＰアドレス認証（Ｓ７０４）、無線基地局認証（Ｓ７０５）を行う。

尚、Ｓ７０３～Ｓ７０５はどのような順番で実行しても良い。

【００８７】

次に制御部１１は、パケット認証、ＩＰアドレス認証、無線基地局認証のうち少なくともいずれか１つの認証処理が成功しているか否かを判定する（Ｓ７０６）。いずれの認証処理も成功していない場合は（Ｓ７０６のＮｏ）、端末５ｃが使用許可範囲外であるため、処理を終了し、シャットダウン等を行う。

いずれかの認証処理が成功した場合は（Ｓ７０６のＹｅｓ）、続いて、ＧＰＳ認証（Ｓ７０７）、電波認証（Ｓ７０８）、光認証（Ｓ７０９）を行う。なお、上述の各認証処理における認証の結果は、パケット受信フラグ、位置情報、電波受信フラグ、光受光フラグ等としてＲＡＭまたは記憶部１２に記憶されるものとする。認証成功の場合は、該当するフラグが「１」にセットされ、認証失敗の場合は該当するフラグが「０」にセットされる。

【００８８】

Ｓ７０９が終了すると、端末５ｃの制御部１１は、認証ＡＰ５５ｃの機能によって、安全指数表２１に設定されている各認証処理の安全指数を認証処理結果を示す各フラグの値（「１」または「０」）に乗じ、安全指数の合計値を求める（Ｓ７１０）。

制御部１１は、安全指数の合計値からセキュリティレベルを判定し（Ｓ７１１）、レベルに応じてＯＳ起動（Ｓ７１２）、機能制限付きＯＳ起動（Ｓ７１３）、或いは使用不可能状態へ端末５ｃを遷移させ、起動処理を終了する。

Ｓ７１０～Ｓ７１３の処理は、第４の実施の形態における図１７のＳ５０７～Ｓ５１０と同様である。

尚、Ｓ７０７～Ｓ７０９の順番はどのような順番で実行しても良い。

【００８９】

例えば、図２５に示すようにパスワード認証、無線基地局認証、光認証が認証成功し、パケット認証、ＩＰアドレス認証、ＧＰＳ認証、電波認証が認証失敗の場合は、安全指数の合計値は「１６」となる。この場合、図１５に示すレベル別起動設定２２に従って、セキュリティレベルは「中」レベルと判定されるため、端末５ｃは機能制限状態で起動される。

尚、Ｓ７０６の判定を行わず、パケット認証、ＩＰアドレス認証、無線基地局認証が全て認証失敗しても、Ｓ７０７以降のＧＰＳ認証、電波認証、光認証を続行し、Ｓ７１１のセキュリティレベル判定を行うようにしてもよい。この場合、ＧＰＳ認証や、正当なユーザに持たせた認証用の電波発信装置６や発光装置７を用いれば、通信設備がない状況下であったり、不具合により通信断が生じてパケット認証ができない状況でも、各種の認証処理を組み合わせて所定機能の使用を可能とでき、様々な使用環境に柔軟に対応できる。

【００９０】

図２６は、第５の実施の形態における端末５ｃの監視処理の詳細を示すフローチャートである。図２６の処理を行う前提として、サーバ３は、管理対象ネットワーク２ａ、２ｃに対して、端末使用許可情報を所定の送信間隔時間ごとに同報送信しているものとする。

【００９１】
Ｓ８０１～Ｓ８０３において、端末５ｃの制御部１１は、監視ＡＰ５６ｃの機能によって、パケット監視、ＩＰアドレス監視、無線基地局監視を行う。
尚、Ｓ８０１～Ｓ８０３はどのような順番で実行しても良い。
【００９２】
次に制御部１１は、パケット監視、ＩＰアドレス監視、無線基地局監視のうち少なくともいずれか１つの監視処理が成功しているか否かを判定する（Ｓ８０４）。いずれの監視処理も成功していない場合は（Ｓ８０４のＮｏ）、端末５ｃが端末使用許可範囲外であるため、処理を終了し、シャットダウン等を行う。
いずれかの監視処理が成功した場合は（Ｓ８０４のＹｅｓ）、続いて、ＧＰＳ監視（Ｓ８０５）、電波監視（Ｓ８０６）、光監視（Ｓ８０７）を行う。なお、上述の各監視処理の結果は、パケット受信フラグ、位置情報、電波受信フラグ、光受光フラグ等としてＲＡＭまたは記憶部１２に記憶されるものとする。監視成功の場合は、該当するフラグが「１」にセットされ、監視失敗の場合は該当するフラグが「０」にセットされる。
【００９３】
Ｓ８０７が終了すると、端末５ｃの制御部１１は、監視ＡＰ５６ｃの機能によって、安全指数表２１に設定されている安全指数を対応する監視処理の結果を示す各フラグの値（「１」または「０」）に乗じ、安全指数の合計値を求める（Ｓ８０８）。
制御部１１は、安全指数の合計値からセキュリティレベルが前回の監視処理時と比較して低下したか否かを判定し（Ｓ８０９）、同じセキュリティレベルを維持している場合（Ｓ８０９のＮｏ）は、制御部１１はＳ８０１に進む。
セキュリティレベルが低下した場合であっても（Ｓ８０９のＹｅｓ）、レベルが「低」でない場合は（Ｓ８１０のＮｏ）、制御部１１は、該当する機能制限状態に端末５ｃを遷移させる（Ｓ８１１）。
セキュリティレベルが低下し（Ｓ８０９のＹｅｓ）、「低」となった場合は（Ｓ８１０のＹｅｓ）、制御部１１は、「低」レベルに該当する状態である使用不可状態に端末５ｃを遷移させる。すなわち、処理を終了し、シャットダウン等を行う。
尚、Ｓ８０５～Ｓ８０８は、どのような順番で実行しても良い。
また、Ｓ８０４の判定を行わず、パケット監視、ＩＰアドレス監視、無線基地局監視が全て失敗しても、Ｓ８０５以降のＧＰＳ監視、電波監視、光監視を続行し、Ｓ８０９のセキュリティレベル判定を行うようにしてもよい。この場合、不具合により通信断が生じてパケット監視等ができない状況でも、ＧＰＳ監視や、正当なユーザに持たせた認証用の電波発信装置６や発光装置７を用いれば、各種の監視が可能となるため、様々な使用環境に柔軟に対応できる。
【００９４】
以上、第５の実施の形態では、管理対象ネットワーク２を拡張し、公衆のネットワークを利用して使用管理システム１ｃを構築した場合にも、第１の実施の形態のパケット認証に加え、ＩＰアドレス認証や無線基地局認証等を行って、端末５ｃが使用許可範囲内にない場合に、その使用を制限できる。例えば、国内の通信事業者を利用して通信接続していれば端末５ｃが国内にあるとして、サーバ３から許可情報を受け取れる状態になくても、所定の機能制限の下で端末５ｃを使用できるようにしたり、逆に、国外へ持ち出していてもサーバ３から許可情報を受信していれば所定の機能制限の下で端末５ｃを使用できるようにしたりすることも可能となる。また、サーバ３からの許可情報を受信せず、登録されていないＩＰアドレスが割り振られている場合や、登録されていない無線基地局に通信接続されている場合には、端末５ｃが明らかに許可されない範囲で使用されたとして、ただちにシャットダウンすることもできるため、盗難された場合でもデータの流出等を防ぐことができる。
【００９５】
尚、前述の説明では、端末５ｃには、記憶部暗号化ＡＰ５４ｃがインストールされるものとしたが、図２７に示すように、第２の実施の形態における検疫ＡＰ５７と同等のプロ

グラム（検疫ＡＰ５７ｃ）をインストールしても良い。この場合、認証ＡＰ５５ｃによって行われる認証の結果、および監視ＡＰ５６ｃによって行われる監視の結果が、実行時刻とともに収集され、定期的にサーバ３に送信される。

【００９６】

第１の実施の形態から第５の実施の形態を通して、サーバ３から同報送信される情報は、端末５（５ａ、５ｂ、５ｃ）の使用を許可することを示す端末使用許可情報とした。しかしながら、本発明はこの例に限定されない。例えば、サーバ３から同報送信される情報としては、端末５（５ａ、５ｂ、５ｃ）の使用を禁止することを示す端末使用禁止情報であっても良い。この場合、使用可能状態の端末５（５ａ、５ｂ、５ｃ）は、端末使用禁止情報を受信すると、使用不可能状態に遷移させる。これによって、例えば、ウィルス感染したコンピュータが管理対象ネットワーク２、２ａ、２ｃに接続されていることを検知した場合などにおいて、管理対象ネットワーク２、２ａ、２ｃに接続されている他の端末５（５ａ、５ｂ、５ｃ）の感染を防ぐことが可能となる。

【００９７】

また、図２０に示すように管理対象ネットワーク２ｃが無線通信ネットワークを含み、無線基地局１３が、端末５ｃの使用を許可することを示す許可情報を間欠的に同報送信することが可能な場合には、端末５ｃは無線基地局１３から同報送信される情報を受信し、無線基地局１３から同報送信される許可情報もパケット認証の対象とする。これによって、端末は無線基地局から同報送信される許可情報を受信して、パケット認証を行えるため、モバイル端末を利用した使用管理システムを安全に構築できるようになる。

【００９８】

以上、添付図面を参照しながら、本発明における使用管理システム等の好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、本願で開示した技術的思想の範疇内において、各種の変更例又は修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【符号の説明】

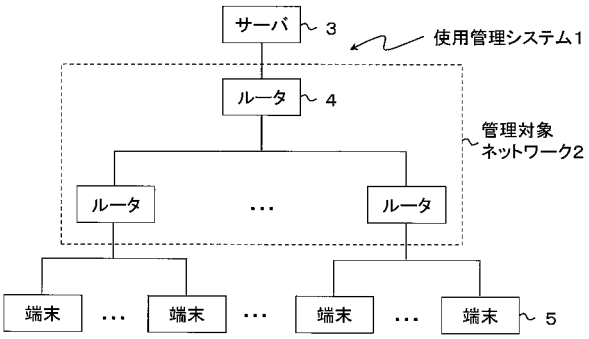
【００９９】

１、１ａ、１ｃ……使用管理システム
２、２ａ、２ｃ……管理対象ネットワーク
３……サーバ
４……ルータ
５、５ａ、５ｂ、５ｃ……端末
６……電波発信装置
７……発光装置
３１……ＢＩＯＳ
３２……ブートローダ
３３……ＯＳ
３４……使用管理ＡＰ
５１……ＢＩＯＳ
５２……ブートローダ
５３……ＯＳ
５４……記憶部暗号化ＡＰ
５５、５５ａ、５５ｂ、５５ｃ……認証ＡＰ
５６、５６ａ、５６ｂ、５６ｃ……監視ＡＰ
５７、５７ｂ、５７ｃ……検疫ＡＰ
６１……セキュリティレベル表
１１……インターネット
１２……ＩＳＰ
１３……無線基地局
１４……ＶＰＮサーバ

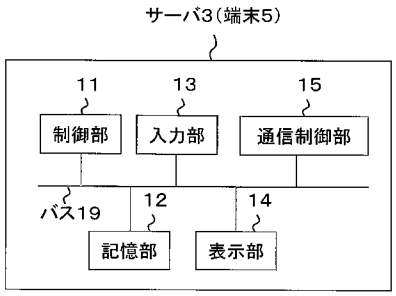
２１、２５……安全指数表
２２……レベル別起動設定

【要約】
【課題】コストをかけず、確実に使用を管理することが可能な使用管理システム等を提供する。
【解決手段】管理対象ネットワーク２は、企業等の単一の管理主体によって管理され、インターネット等の外部ネットワークに対して閉じているネットワークである。サーバ３は、管理対象ネットワーク２に対して、端末５の使用を許可することを示す端末使用許可情報を所定の送信間隔時間ごとに同報送信する。端末５は、サーバ３から同報送信される情報を受信し、端末使用許可情報を受信した場合にはパケット認証成功とする。更に他の種類の認証処理を実行し、それらの認証結果と予め設定された安全指数に応じてセキュリティレベルを判定し、セキュリティレベルに応じて使用可、機能制限付き使用可、或いは使用不可のいずれかの状態に遷移する。
【選択図】図１７

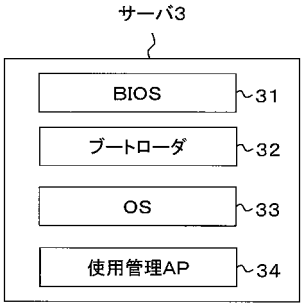
【図１】



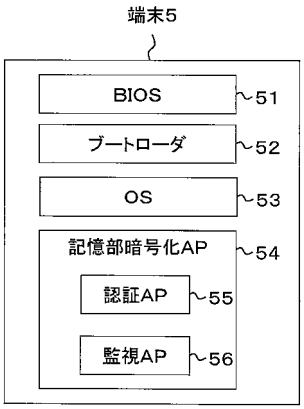

【図２】



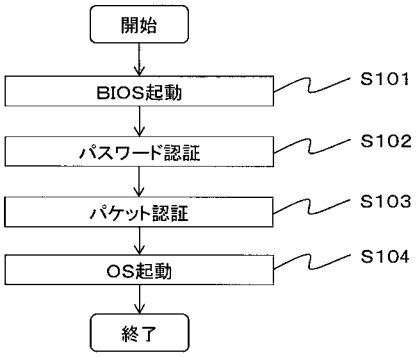

【図３】



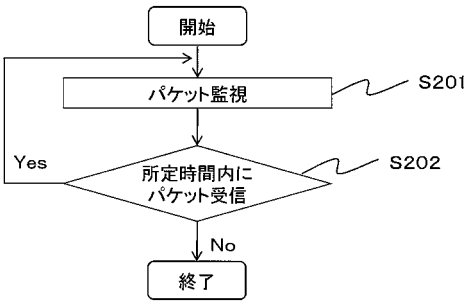

【図４】



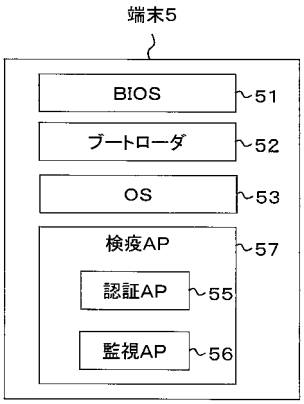
【図５】



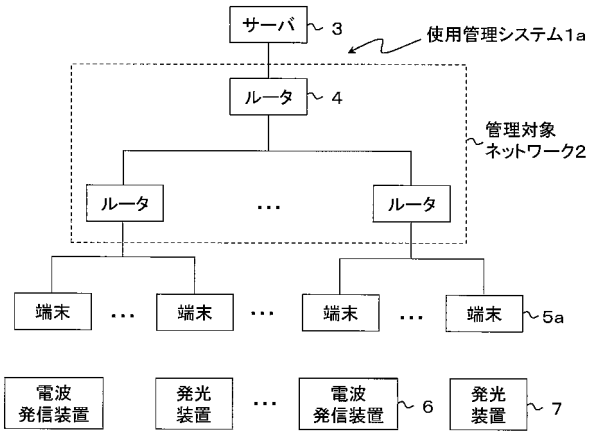

【図６】



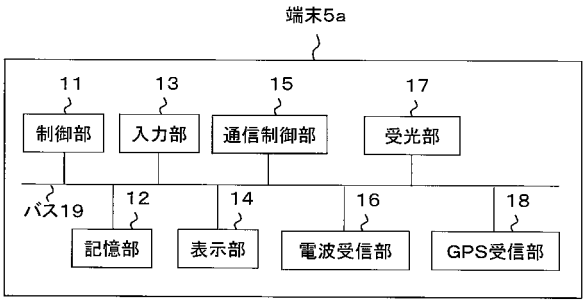

【図７】



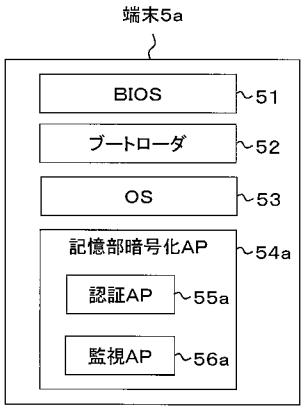

【図８】




【図９】




【図１０】

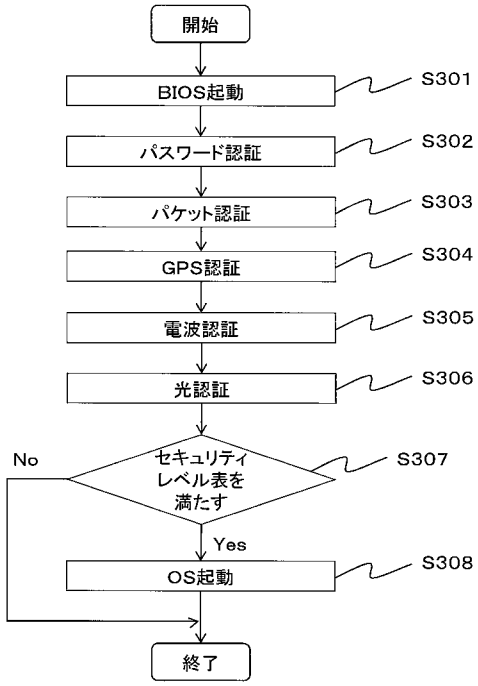



【図１１】

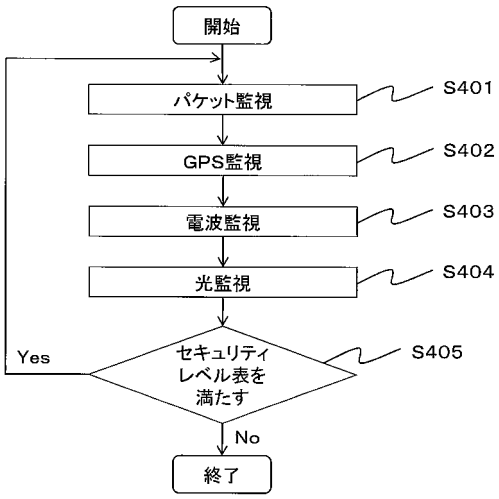
セキュリティレベル表61

| | レベル1 | レベル2 | レベル3 | レベル4 | レベル5 |
|---|---|---|---|---|---|
| パスワード認証 | 要 | 要 | 要 | 要 | 要 |
| パケット認証(監視) | 不要 | 要 | 要 | 要 | 要 |
| GPS認証(監視) | 不要 | 不要 | 要 | 要 | 要 |
| 電波認証(監視) | 不要 | 不要 | 不要 | 要 | 要 |
| 光認証(監視) | 不要 | 不要 | 不要 | 不要 | 要 |

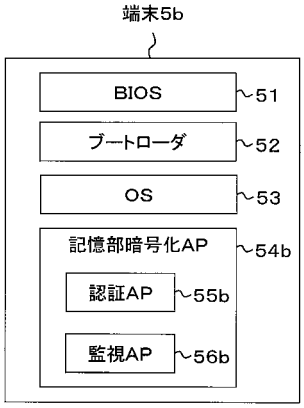
【図１２】




【図１３】




【図１４】




【図１５】

安全指数表21

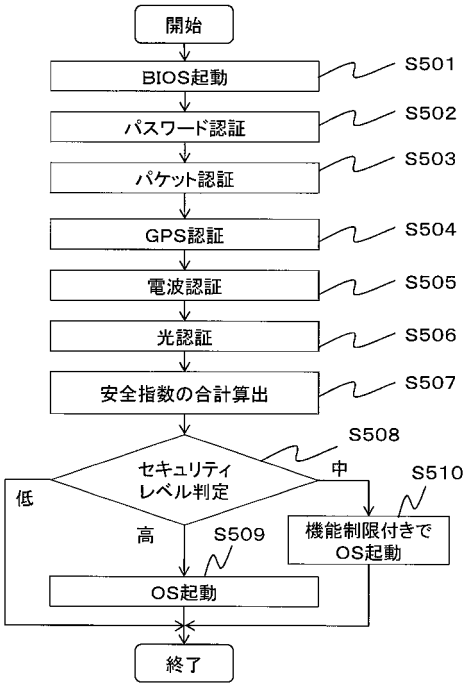
| | 安全指数 |
|---|---|
| パケット認証 | 5 |
| GPS認証 | 4 |
| 電波認証 | 7 |
| 光認証 | 7 |
| ⋮ | ⋮ |

【図１６】

レベル別起動設定22

| 安全指数の合計値 | セキュリティレベル | 状態 |
|---|---|---|
| 0～10 | 低 | 使用不可 |
| 11～20 | 中 | 機能制限付き使用可 |
| 21以上 | 高 | 使用可 |

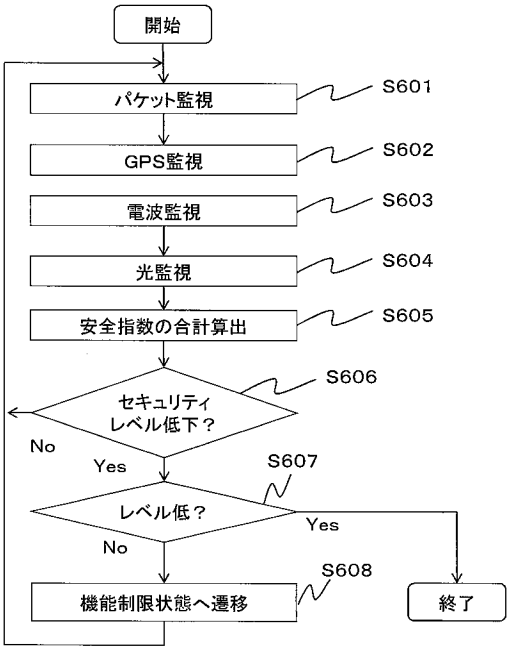
【図１７】



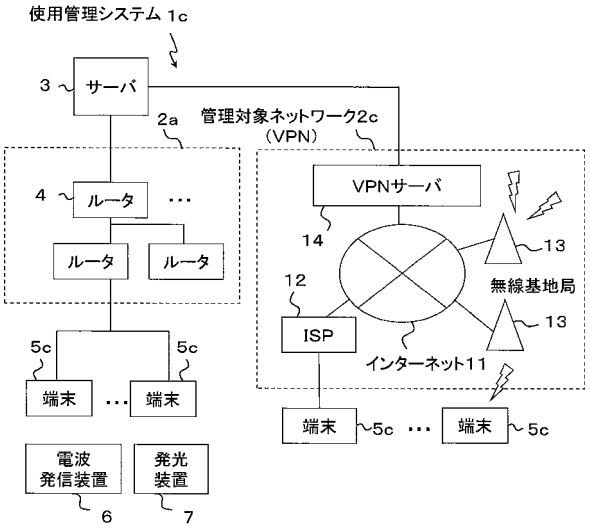

【図１８】

| | OK／NG | 安全指数 |
|---|---|---|
| パスワード認証 | OK | 5 |
| パケット認証（監視） | OK | 5 |
| GPS認証（監視） | NG | 0 |
| 電波認証（監視） | OK | 7 |
| 光認証（監視） | OK | 7 |
| 合計 | — | 24 |

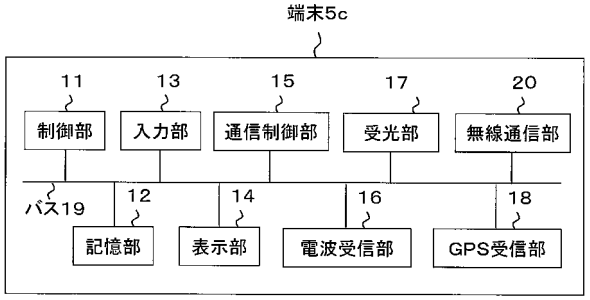
【図１９】



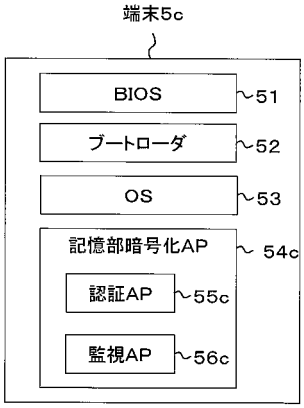

【図２０】




【図２１】



【図２２】

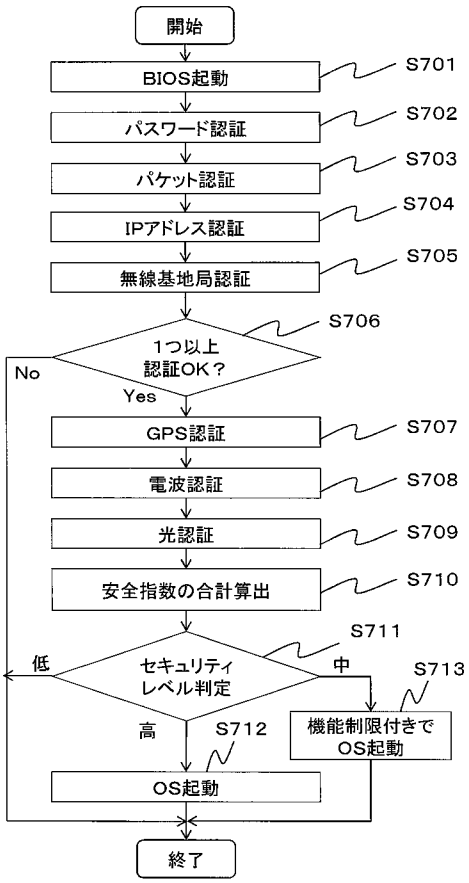



【図２３】

安全指数表25

| | 安全指数 |
|---|---|
| パスワード認証 | 5 |
| パケット認証 | 5 |
| IPアドレス認証 | 4 |
| 無線基地局認証 | 4 |
| GPS認証 | 4 |
| 電波認証 | 7 |
| 光認証 | 7 |
| ⋮ | ⋮ |

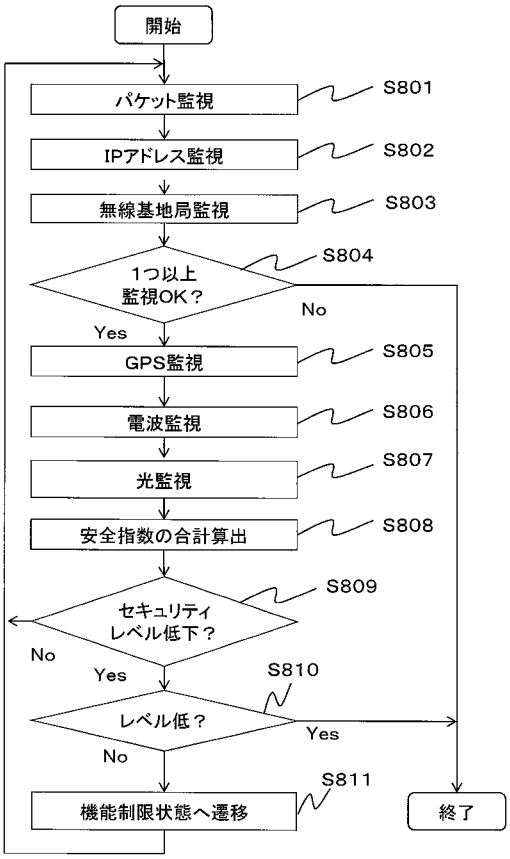
【図２４】



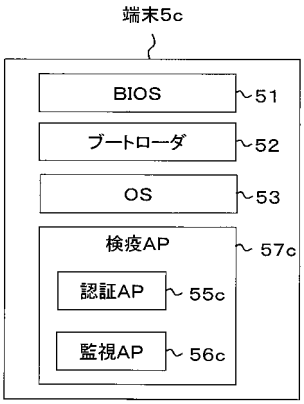

【図２５】

| | OK／NG | 安全指数 |
|---|---|---|
| パスワード認証 | OK | 5 |
| パケット認証（監視） | NG | 0 |
| IPアドレス認証（監視） | NG | 0 |
| 無線基地局認証（監視） | OK | 4 |
| GPS認証（監視） | NG | 0 |
| 電波認証（監視） | NG | 0 |
| 光認証（監視） | OK | 7 |
| 合計 | — | 16 |

【図２６】


開始
パケット監視
S801
IPアドレス監視
S802
無線基地局監視
S803
1つ以上
監視OK？
S804
No
Yes
GPS監視
S805
電波監視
S806
光監視
S807
安全指数の合計算出
S808
セキュリティ
レベル低下？
S809
No
Yes
レベル低？
S810
Yes
No
機能制限状態へ遷移
S811
終了

【図２７】


端末5c
BIOS
51
ブートローダ
52
OS
53
検疫AP
57c
認証AP
55c
監視AP
56c

フロントページの続き

(72)発明者　馬　天峰
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内
(72)発明者　木下　惇
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内
(72)発明者　栗原　良輔
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内
(72)発明者　緑川　純央
東京都千代田区丸の内一丁目６番５号　株式会社野村総合研究所内

審査官　市川　武宜

(56)参考文献　特開平１１－３０６１４２（ＪＰ，Ａ）
特開２０００－２７６２４７（ＪＰ，Ａ）
特開２００７－２９９０３４（ＪＰ，Ａ）
特開２００７－１０２４４０（ＪＰ，Ａ）
特開２００１－０８４１７４（ＪＰ，Ａ）
特開２００９－１５１４９９（ＪＰ，Ａ）
特開平０５－１５０８５３（ＪＰ，Ａ）
特開２００３－０９９４００（ＪＰ，Ａ）
特開２００６－２６８３２５（ＪＰ，Ａ）
特開２００８－１５９０２４（ＪＰ，Ａ）
特開２００７－１１６５０９（ＪＰ，Ａ）
特開２００７－２５７０６６（ＪＰ，Ａ）
特開２００３－２８８２７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｇ０６Ｆ　２１／２４
Ｈ０４Ｌ　９／３２