(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開2002－63140

（P2002－63140A）

(43)公開日　平成14年２月28日(2002.2.28)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00　３３０Ｅ	５Ｂ０１７
		３３０Ｂ	５Ｂ０８２
12/00	５３７	12/00　５３７Ｄ	５Ｂ０８５
12/14	３２０	12/14　３２０Ｂ	５Ｊ１０４
		３２０Ｃ	

審査請求　有　請求項の数24　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願2001－170345(P2001－170345)

(22)出願日　平成13年６月６日(2001.6.6)

(31)優先権主張番号　０９／５８９７４７

(32)優先日　平成12年６月９日(2000.6.9)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　591169755
ティーアールダブリュー・インコーポレーテッド
ＴＲＷ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国オハイオ州44124，リンドハースト，リッチモンド・ロード　1900

(72)発明者　ニール・ジー・シーゲル
アメリカ合衆国カリフォルニア州，ランチョ・パロス・ヴァーデス

(74)代理人　100089705
弁理士　社本　一夫　（外５名）

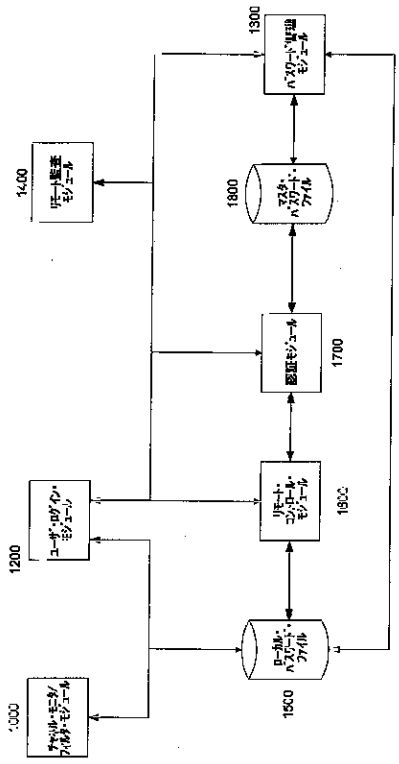
最終頁に続く

(54)【発明の名称】　ネットワーク上のアクセス管理方法及びシステム

(57)【要約】

【課題】ネットワーク上のアクセス及びセキュリティを管理する。

【解決手段】ローカル・パスワード・ファイル１５００は、ネットワーク上の全てのコンピュータに備えられ、ネットワークへのアクセスが許可されている正規ユーザの、ユーザＩＤ、一方向暗号化パスワード、及び特権を記憶する。ユーザ・ログイン・モジュール１２００は、ユーザからユーザＩＤ又は役割及びパスワードを受信し、ファイル１５００中に一致するものがある場合に、ユーザをログインする。チャネル・モニタ／フィルタ・モジュール１０００は、ネットワーク上のメッセージを監視／受信し、ユーザの特権がメッセージの視認を許可する場合、ユーザ端末にメッセージを表示する。パスワード管理モジュール１３００は、全てのファイル１５００を更新して、同一内容にする。リモート監査モジュール１４００は、ユーザ端末上で発生する異常事態を監視し処理する。



【特許請求の範囲】
【請求項１】　複数のコンピュータを有するネットワークにおけるアクセス及びセキュリティを管理する方法であって、
ネットワーク中の複数のコンピュータの各々に、複数のコンピュータ及びネットワークに対するアクセスが許可されている正規のユーザ端末に関する、複数のユーザ識別（ＩＤ）と、複数の一方向暗号化パスワードと、複数の付随特権とを格納している一方向暗号化パスワード・ファイルをインストールするステップと、
ユーザがネットワーク上の複数のコンピュータの１つにログインしようとするとき、ユーザにより入力されたパスワードを一方向暗号化するステップと、
ユーザにより入力されたユーザＩＤ及び一方向暗号化されたパスワードと、一方向暗号化パスワード・ファイル内に格納されている複数のユーザＩＤ及び複数の一方向暗号化パスワードとの間に、一致するものがあるかどうかを判定するステップと、
一方向暗号化パスワード・ファイル中に一致するものが存在する場合、ユーザの付随特権によって許可される、コンピュータ及びネットワーク上に格納されているデータ及びソフトウエアに対するアクセスをイネーブルするステップと、
一方向暗号化パスワード・ファイル中に一致するものが存在する場合、付随特権によって許可されるメッセージをフィルタリングし、該メッセージをユーザに表示するステップとからなることを特徴とする方法。
【請求項２】　請求項１記載の方法において、一方向暗号化パスワード・ファイルに格納されている付随特権は、コンピュータ、ネットワークに含まれ、かつネットワーク上を送信されるソフトウエア、データ、及びメッセージに対するアクセスについて、ユーザＩＤのセキュリティ・レベル及びアクセス特権を表していることを特徴とする方法。
【請求項３】　請求項１記載の方法において、ユーザがユーザＩＤ及び一方向暗号化されるパスワードを入力しようとして、一方向暗号化パスワード・ファイル内に格納されている複数のユーザＩＤ及び一方向暗号化パスワードと少なくとも１回一致しなかった場合、該方法は、更に、
コンピュータを介して、システム管理者又はセキュリティ担当者に、一方向暗号化パスワード・ファイルに格納されているユーザＩＤ及び一方向暗号化パスワードに一致する、ユーザＩＤ及び一方向暗号化パスワードをユーザが提示できない旨の通知を送信するステップを含むことを特徴とする方法。
【請求項４】　請求項３記載の方法において、該方法は更に、
システム管理者又はセキュリティ担当者によって要求されたときに、ユーザＩＤ及び一方向暗号化パスワードの入力の試行において少なくとも１回失敗したユーザがアクセスしようとするコンピュータをロックし、ユーザにログイン画面に対するアクセスだけを許可するステップを含むことを特徴とする方法。
【請求項５】　請求項３記載の方法において、
該方法は更に、システム管理者又はセキュリティ担当者によって要求されたときに、ユーザを欺いてコンピュータに対するアクセスが許可されたと信じさせるステップを含み、
欺くステップは、ユーザに対する偽メッセージ及び情報の提示を含むことを特徴とする方法。
【請求項６】　請求項３記載の方法において、該方法は更に、
システム管理者又はセキュリティ担当者によって要求されたときに、コンピュータ・システムをディスエーブルし、ユーザが当該コンピュータ・システムにアクセスできないようにするステップを含むことを特徴とする方法。
【請求項７】　請求項１記載の方法において、該方法は更に、
複数のコンピュータ中のあるコンピュータにおいて異常事態を検出するステップと、
異常事態をシステム管理者又はセキュリティ担当者に報告するステップとを含むことを特徴とする方法。
【請求項８】　請求項７記載の方法において、異常事態は、
ユーザのログイン試行の失敗回数が許容可能な回数を超過したこと、
ユーザの付随特権に変更があったこと、
ユーザによって、システム・ディスエーブル動作が開始されたこと、
ユーザのパスワードが期限切れとなったこと、
無効のデジタル署名により、メッセージが拒絶されたこと、
リモート・ユーザの再認証要求が、システム管理者又はセキュリティ担当者によって受信されたこと、
リモート・ユーザの締め出し要求が、システム管理者又はセキュリティ担当者によって受信されたこと、及びシステム管理者又はセキュリティ担当者において、リモート・ローディング・パスワードの要求が無事完了したことを含むことを特徴とする方法。
【請求項９】　請求項７記載の方法において、該方法は更に、
システム管理者又はセキュリティ担当者によって要求されたとき、又はユーザによって即時停止が要求されたとき、異常事態に応答して、コンピュータ上の複数のファイルを削除し、コンピュータをディスエーブルするステップを含むことを特徴とする方法。
【請求項１０】　請求項８記載の方法において、該方法は更に、

異常事態が発生したときに、コンピュータ・システムをディスエーブルするか、又はユーザを欺くか、又はコンピュータ・システムをロックするかを実行するステップを含むことを特徴とする方法。

【請求項１１】　複数のコンピュータを有するネットワーク上においてアクセス及びセキュリティを管理するシステムであって、
ネットワーク中の複数のコンピュータの各々に存在する一方向暗号化パスワード・ファイルであって、複数のコンピュータ及びネットワークに対するアクセスが許可されている正規のユーザに関する、複数のユーザ識別、関連する一方向暗号化パスワード、及び付随特権を含んでいる、一方向暗号化パスワード・ファイルと、
ユーザからユーザＩＤ又は役割及びパスワードを受信し、一方向暗号化パスワード・ファイル中にこれらと一致するものが見出されたときに、ユーザをログインする、ユーザ・ログイン・モジュールと、
ネットワーク内においてブロードキャスト又はマルチキャスト・メッセージを監視しかつ受信し、ユーザの付随特権がメッセージの視認を許可する場合、メッセージをユーザに表示する、チャネル・モニタ／フィルタ・モジュールとを備えることを特徴とするシステム。

【請求項１２】　請求項１１記載のシステムにおいて、該システムは更に、
ネットワーク内のコンピュータが全て、同じ一方向暗号化パスワード・ファイルを収容するように該ファイルを更新し、これを確実にするパスワード管理モジュールを備えることを特徴とするシステム。

【請求項１３】　請求項１１記載のシステムにおいて、該システムは更に、
コンピュータ上で発生し得る異常事態を監視し処理するリモート監査モジュールを備えることを特徴とするシステム。

【請求項１４】　請求項１３記載のシステムにおいて、異常事態は、
ユーザのログイン試行失敗回数が許容可能な失敗回数を超過したこと、
ユーザの付随特権に変更があったこと、
ユーザによって、システム・ディスエーブル動作が開始されたこと、
ユーザのパスワードが期限切れとなったこと、
無効のデジタル署名により、メッセージが拒絶されたこと、
リモート・ユーザの再認証要求が、システム管理者又はセキュリティ担当者によって受信されたこと、
リモート・ユーザの締め出し要求が、システム管理者又はセキュリティ担当者によって受信されたこと、及びシステム管理者又はセキュリティ担当者において、リモート・ローディング・パスワードの要求が無事完了したことを含むことを特徴とするシステム。

【請求項１５】　請求項１１記載のシステムにおいて、該システムは更に、
異常事態が発生したとき、システム管理者又はセキュリティ担当者に適切な処置を取らせるリモート・コントロール・モジュールを備えていることを特徴とするシステム。

【請求項１６】　請求項１５記載のシステムにおいて、適切な処置は、
システム管理者又はセキュリティ担当者によって要求されたときに、コンピュータ・システムをディスエーブルし、ユーザがコンピュータ・システムにアクセスできないようにすること、及びシステム管理者又はセキュリティ担当者によって要求されたときに、コンピュータに格納されている複数のファイルを削除することを含むことを特徴とするシステム。

【請求項１７】　請求項１１記載のシステムにおいて、該システムは更に、
ユーザＩＤ及びパスワードを、システム管理者又はセキュリティ担当者によってアクセス可能なコンピュータに格納されているマスタ・パスワード・ファイルに突き合せてチェックすることによって、ユーザ・ログイン・モジュールが、コンピュータ内に収容されている一方向暗号化パスワードにおいて一致を見出した後、ユーザを再認証するための認証モジュールを備えることを特徴とするシステム。

【請求項１８】　請求項１２記載のシステムにおいて、パスワード管理モジュールは、完全なユーザＩＤ、一方向暗号化パスワード、及び付随特権を含むマスタ・パスワード・ファイルをメッセージに添付し、システム管理者及びセキュリティ担当者の秘密キー及びパスフレーズを用いてメッセージを暗号化し、該メッセージを全ユーザにブロードキャストするよう構成されていることを特徴とするシステム。

【請求項１９】　コンピュータにより実行可能であり、コンピュータ読み取り可能媒体内に記憶され、複数のコンピュータを有するネットワーク上においてアクセス及びセキュリティを管理するコンピュータ・プログラムであって、
ネットワーク内の複数のコンピュータそれぞれに備えられる一方向暗号化パスワード・ファイルであって、複数のコンピュータ及びネットワークに対するアクセスを許されている正規のユーザに関する、複数のユーザＩＤ、一方向暗号化パスワード、及び付随特権を含んでいる一方向暗号化パスワード・ファイルと、
ユーザからユーザＩＤ又は役割及びパスワードを受信し、一方向暗号化パスワード・ファイル中にこれらと一致するものが見出されたとき、ユーザをログインさせるユーザ・ログイン・コード・セグメントと、
ネットワーク内においてブロードキャスト・メッセージ又はマルチキャスト・メッセージを監視しかつ受信し、

ユーザの付随特権がメッセージの視認を許可する場合、メッセージをユーザに表示するチャネル・モニタ／フィルタ・コード・セグメントとを備えることを特徴とするコンピュータ・プログラム。

【請求項２０】　請求項１９記載のコンピュータ・プログラムにおいて、該プログラムは更に、
ネットワークのコンピュータ全てが同一の一方向暗号化パスワード・ファイルを収容するように該ファイルを更新し、これを確実にするパスワード管理コード・セグメントを備えることを特徴とするコンピュータ・プログラム。

【請求項２１】　請求項１９記載のコンピュータ・プログラムにおいて、該プログラムは更に、
コンピュータ上で発生し得る異常事態を監視し処理するリモート監査コード・セグメントを備えることを特徴とするコンピュータ・プログラム。

【請求項２２】　請求項２１記載のコンピュータ・プログラムにおいて、異常事態は、
ユーザのログイン試行失敗回数が許容可能な回数を超過したこと、
ユーザの付随特権に変更があったこと、
ユーザによって、システム・ディスエーブル動作が開始されたこと、
ユーザのパスワードが期限切れとなったこと、
無効のデジタル署名により、メッセージが拒絶されたこと、
リモート・ユーザの再認証要求が、システム管理者又はセキュリティ担当者によって受信されたこと、
リモート・ユーザの締め出し要求が、システム管理者又はセキュリティ担当者によって受信されたこと、及びシステム管理者又はセキュリティ担当者において、リモート・ローディング・パスワードの要求が無事完了したことを含むことを特徴とするコンピュータ・プログラム。

【請求項２３】　請求項１９記載のコンピュータ・プログラムにおいて、該プログラムは更に、
異常事態が発生したとき、システム管理者又はセキュリティ担当者に適切な処置を取らせるリモート・コントロール・コード・セグメントを備えていることを特徴とするコンピュータ・プログラム。

【請求項２４】　請求項１９記載のコンピュータ・プログラムにおいて、該プログラムは更に、
ユーザＩＤ及びパスワードを、システム管理者又はセキュリティ担当者によってアクセス可能なコンピュータに格納されているマスタ・パスワード・ファイルに突き合せてチェックすることによって、ユーザ・ログイン・モジュールが、コンピュータ内に収容されている一方向暗号化パスワードにおいて一致を見出した後、ユーザを再認証するための認証コード・セグメントを備えることを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高い可用性、セキュリティ及び残存力（ｓｕｒｖｉｖａｂｉｌｉｔｙ）を可能にするネットワーク・アクセス制御システム及び方法に関する。更に特定すれば、本発明は、アクセス及び制御に関係する通信上の通信トラフィックを最少に抑えつつ、低帯域幅通信媒体によって分散ネットワークに対するアクセス及び制御を可能にするシステム、方法及びコンピュータ・プログラムを採用する。なお、本発明は、米国陸軍によって裁定された契約番号ＤＡＡＢ０７－９５－Ｄ－Ｅ６０４の下で、政府の援助を受けて行われたものであり、米国政府は、本発明において、相応の権利を有する。

【０００２】

【従来の技術】比較的短いコンピュータ産業の歴史において、劇的な変化が生じてきた。これらの変化の内、最も重要な変化は、ハードウエア価格の信じがたい急落、及びコンピュータ・ハードウエアの性能、信頼性、サイズ及び堅牢性に関する大幅な改善である。コンピュータの信頼性及び性能は、軍がコンピュータを個々の戦闘車両各々に搭載可能なことろまで向上している。このように、コンピュータのワイド・エリア・ネットワークが形成され、命令や、敵及び援軍の位置、その移動のような、任務に重要なその他のデータを受信するために用いられる場合がある。しかしながら、このようなワイド・エリア・ネットワーク上でセキュリティを実現するのは、困難な場合がある。多くの課題の１つに、ネットワークが取り得るシアー・サイズ（ｓｈｅｅｒ　ｓｉｚｅ）がある。様々なタイプのコンピュータの数千ものノードがネットワークにアクセスする場合がある。

【０００３】更に、殆どのユーザは、ネットワーク上で送信されるデータの一部しか受信することを許されていない場合もある。更にまた、ネットワークは戦場で動作する場合もあるので、高速通信を可能にするケーブルの使用は問題外である。無線及びマイクロ波通信方法のみ、直接的に又は衛星システムを経由して利用することができる。しかしながら、無線及びマイクロ波通信の使用では、ネットワーク上でのデータ伝送速度に限界がある。高速ケーブルを用いたネットワークを利用する場合でも、ネットワーク上のノード数が膨大なために、管理用データ・トラフィックを絶対的な最少限に止めることは、避けることができない。

【０００４】通信の問題に加えて、セキュリティの問題が重要である。戦場においてシステムにアクセスする兵隊の殆どは、ネットワークを通じて伝達される情報の殆どを受信することを許可されていない。ネットワーク上において個々の人に認められているのは類別された情報を受信することであり、全員が同じセキュリティ・クリアランス・レベルにある訳ではない。したがって、ネットワークをマルチレベル・セキュリティ・システムに区

分する機構が提案され試行されている。しかしながら、これらのマルチレベル・システムは、複雑で高価なことが多く、適正に機能するためには大量の帯域幅が利用可能でなければならず、しかも管理するにはかなりのマン・パワーが集中的に必要となる。したがって、比較的低い帯域幅の通信システム上で、戦場においてこのようなマルチレベル・セキュリティ・システムを実現することは、極めて困難である。更に、戦闘では、車両が捕獲される可能性があるため、このようなシステムの実現は一層難しくなる。敵が我軍の戦闘計画や部隊の移動を傍受ことが可能になると、戦闘において敵に圧倒的に有利になってしまう。

【０００５】大きなワイド・エリア・ネットワークを実現するにあたって軍部が直面する上記の問題は、数万人の従業員を有し、全員が専用のパーソナル・コンピュータを有しワイド・エリア・ネットワーク上で世界規模で接続されている大企業にも当てはまる。企業内の従業員は、その殆どが戦場における兵隊と同じカテゴリに該当する。即ち、殆どの従業員がワイド・エリア・ネットワーク上の情報全てにアクセスする必要性はなく、またその要求もない。更に、殆どの企業は、国内及び国外双方に競合を有し、他の企業が開発中の新製品や、発行する入札に関する内部情報が得られれば、有利になるであろう。したがって、軍及び商業分野双方において、権限のある人員に必要な情報に素早くしかも容易にアクセスさせることができ、一方、不正者のアクセスを阻止することは、極めて重大である。

【０００６】これら不正者には、敵の部隊、競合、又は、出没するハッカが含まれる。最近における社内コンピュータのサービス拒否の試みや、電子メール・ビールス／ワームの内部ふるいわけによって注目されているように、無駄な手間や貴重な情報の喪失のために、何十億ドルもの業務コストが、ハッカによって発生する可能性がある。更に、ハッカ又は不平不満を持っている従業員が顧客のクレジット・カード（又は同様の）情報にアクセスし、それをワールド・ワイド・ウェブ上で公開することにより、会社が破滅に至る可能性もある。

【０００７】マルチレベル・セキュリティ・システムの使用以外で、セキュリティを備える主要な方法は、パスワード・アクセス方法の使用によると考えられてきた。このようなパスワードに基づくシステムでは、ユーザに対応する適正なパスワードが入力されない場合、ユーザはコンピュータ・システム又はネットワークへのアクセスを拒否される。通常、ローカル・エリア・ネットワークにおけるサーバ上には単一のパスワード・ファイルが格納されており、当該ローカル・エリア・ネットワーク上における特定のコンピュータ・システムの起動時に、ユーザＩＤ及びパスワードが、サーバ内のそれらと照合される。これは、潜在的ユーザの数が比較的小さく、かなりの帯域幅が使用可能でユーザが同時にログオンすることができる場合には、好適に作用する。

【０００８】しかしながら、多数のユーザが同時にシステムにログオンしようとした場合、単一のパスワード・ファイルに対するアクセスが、システムにおけるボトルネックすなわち隘路となる。更に、アクセスを得る際に、ユーザが常にネットワーク上の単一のサーバにログインしなければならないために、サーバが単独の故障ポイントとなる。したがって、故障が発生すると、ネットワーク全域にわたってユーザが締め出される恐れがある。従来より、ユーザのパスワードは、クリア・テキストすなわち暗号化されていない平文で、ネットワークを通じてサーバに転送されており、この場合、パスワードは敵によって発見され易い。あるいは、伝送中パスワードを暗号化し、サーバ上では平文でセーブする場合もあるが、この場合、サーバは、従来の戦争、ならびに軍及び営利企業双方に適用可能なサイバー戦争にとって、戦場における目標となる。

【０００９】

【発明が解決しようとする課題】大型のネットワークにおけるボトルネックの形成を軽減するために、個々のユーザのパスワードをユーザのローカル・マシン上に格納することが試行されている。個々のコンピュータの起動時に、ユーザは、彼に割り当てられたコンピュータ・システムにログオンし、彼のパスワードを入力する。かかるパスワードを与えないと、個々のコンピュータへのアクセスが禁止される。これによって、中央のパスワード・ファイルに関連するオーバーヘッドがなくなるが、各ユーザは、ネットワーク上で彼らに割り当てられた特定のコンピュータのみが使用可能となるよう制約される。したがって、コンピュータが故障した場合、従業員は別の従業員のコンピュータを用いて、彼に割り当てられた作業を完成させることはできない。このため、リソースが無駄になる。

【００１０】したがって、セキュリティを実現するために必要な管理的通信トラフィックを絶対的な最少限に止めつつ、ローカル・エリア・ネットワーク及びワイド・エリア・ネットワークに高度のセキュリティを備えるシステム、方法、及びコンピュータ・プログラムの提供が求められている。更に、このようなシステム、方法、及びコンピュータ・プログラムは、不正ユーザや、適正なセキュリティ許可がないユーザに対して、アクセスを阻止しなくてはならない。加えて、ユーザは、ネットワーク内のあらゆるコンピュータ・システムにログオンすることができ、更に特定のユーザ又は彼の組織における役割のために、メッセージを受信し情報にアクセスすることができなければならない。また、セキュリティ・システムは、不正ユーザがネットワーク上の特定のコンピュータに対する完全なアクセスが可能であっても、不正ユーザが、システム上のその他のユーザのパスワードにアクセスすることを防止しなければならない。また、セキ

ュリティ・システムは、セキュリティ担当者又はシステム管理者が、不正ユーザの手に落ちた（又は落ちたと疑われる）コンピュータを、遠隔制御によりディスエーブルすることが可能でなければならない。

【００１１】

【課題を解決するための手段】本発明の一実施形態は、多数のコンピュータを有するネットワーク上においてアクセス及びセキュリティを管理する方法を提供する。この方法は、開始すると、ネットワーク内の各コンピュータに、一方向暗号化パスワードを含んだローカル・パスワード・ファイルをインストールする。このローカル・パスワード・ファイルは、ネットワーク上のコンピュータに対するアクセスが許可されている正規の各ユーザに、数個のユーザ識別（ＩＤ）、一方向暗号化パスワード、及び付随特権を含んでいる。ユーザが入力した一方向暗号化パスワードは、パスワード・ファイル内に格納されている一方向暗号化パスワードと突き合せてチェックされる。一方向暗号化パスワードを収容するパスワード・ファイル上で一致が見出された場合、コンピュータ及びネットワーク上に収容されているデータ及びソフトウエアの内、ユーザの付随特権によって許可される部分に対するアクセスが可能となる。一方向暗号化パスワードを収容するパスワード・ファイル上で一致が見出されると、フィルタリングが行われ、付随特権によって許されるメッセージをユーザに表示する。

【００１２】更に、本発明の一実施形態は、数個のコンピュータを有するネットワーク上においてアクセス及びセキュリティを管理するシステムを提供する。このシステムは、ネットワーク上の各コンピュータが、一方向暗号化パスワードを含むパスワード・ファイルを有する。パスワード・ファイルは、ネットワーク上のコンピュータに対するアクセスを許されている正規の各ユーザに、数個のユーザＩＤ、関連する（一方向暗号化）パスワード、及び付随特権を含んでいる。また、このシステムは、ユーザ・ログイン・モジュールも有し、ユーザからユーザＩＤ又は役割、及びパスワードを受信し、一方向暗号化パスワードを収容するパスワード・ファイル内において一致が見出された場合、ユーザをログインする。更にまた、このシステムは、チャネル・モニタ／フィルタ・モジュールも有し、ネットワーク内におけるブロードキャスト・メッセージ又はマルチキャスト・メッセージを監視し受信し、ユーザの付随特権がメッセージの取得を許可している場合、ユーザにメッセージを表示する。

【００１３】更にまた、本発明の一実施形態は、コンピュータによる実行が可能であり、コンピュータ読み取り可能媒体上に記憶され、数個のコンピュータを有するネットワーク上においてアクセス及びセキュリティを管理するコンピュータ・プログラムである。このコンピュータ・プログラムは、ネットワーク内の各コンピュータ上に、一方向暗号化パスワードを含むパスワード・ファイルを有する。一方向暗号化パスワード・ファイルは、ネットワーク上のコンピュータに対するアクセスが許可されている正規の各ユーザ毎に、数個のユーザＩＤ、関連する（一方向暗号化）パスワード、及び付随特権を含む。このコンピュータ・プログラムは、更に、ユーザ・ログイン・コード・セグメントも有し、ユーザからユーザＩＤ又は役割（role）、及びパスワードを受信し、一方向暗号化パスワードを収容するパスワード・ファイル内において一致が見出された場合、ユーザをログインする。更にまた、コンピュータ・プログラムは、チャネル・モニタ／フィルタ・コード・セグメントも有し、ネットワーク内におけるブロードキャスト・メッセージ又はマルチキャスト・メッセージを監視し受信し、ユーザの付随特権がメッセージの視認を許可している場合、ユーザにメッセージを表示する。

【００１４】

【発明の実施の形態】本発明は、以下の例示としての実施形態の詳細な説明及び特許請求の範囲を添付図面に関連付けて読むことにより、明白に理解されるであろう。これらは全て、本発明の開示の一部をなすものである。本明細書及び図面の開示は、本発明の実施形態の例を開示することを目的とするが、これらは例示及び一例に過ぎず、本発明はこれらに限定されるのではないことは、明白に理解されるはずである。本発明の技術的思想及び範囲は、添付の特許請求の範囲によってのみ限定されるものである。本明細書及び図面においては、同一の構成要素、対応する構成要素、又は同様の構成要素を示す際に、同様の参照番号及び文字を用いることとする。更に、以下に続く詳細な説明では、一例としてサイズ／モデル／値／範囲を示す場合があるが、本発明はこれらに限定される訳ではない。

【００１５】図1は、軍環境において実現したワイド・エリア・ネットワーク１０の一例を示している。しかしながら、本発明の実施形態は、あらゆる商用ローカル・エリア・ネットワーク及びワイド・エリア・ネットワーク上においても実現可能であり、利用可能であることを注記しておく。図1において、ワイド・エリア・ネットワーク１０は、種々の軍用車両３０を有するものとして示されている。軍用車両３０の各々は、少なくとも１つのプロセッサを用いたシステムを内蔵し、これを用いて、ワイド・エリア・ネットワーク１０にアクセスすることができる。このプロセッサを用いたシステムは、パーム・コンピュータ（ｐａｌｍ　ｃｏｍｐｕｔｅｒ）、パーソナル・デジタル・アシスタント（ＰＤＡ）、ラップトップ・コンピュータ、又はパーソナル・コンピュータとすることができるが、これらに限定される訳ではない。

【００１６】軍用車両３０に加えて、これら軍用車両３０の内の１台を、旅団執行官（Ｂｄｅ　ＸＯ）車両、す

なわちシステム管理者又はセキュリティ担当者（ＳＡ／ＳＯ）車両４０に指定している。すなわち、システム管理者又はセキュリティ担当者のコンピュータ・システムは、軍用車両３０内に装備される任意のユーザ端末上にも配置できる。しかしながら、ＳＡ／ＳＯコンピュータ・システムは、戦闘エリアから離れたところにある構造体５０内に配置されることが通常である。構造体５０及びワイド・エリア・ネットワーク１０間の通信は、無線周波数信号７０を通じて、直接的に又は衛星６０を経由して行われる。更に、ワイド・エリア・ネットワーク１０内部には、任意数の下位ネットワーク２０を含ませることも可能である。

【００１７】先に論じたように、図１に示すワイド・エリア・ネットワーク１０は、戦場環境における使用にも、無線通信にも限定する必要はない。ワイド・エリア・ネットワーク１０は、企業によって商用に用いられるローカル・エリア・ネットワーク又はワイド・エリア・ネットワークとすることができ、同軸ケーブル、光ファイバ・ケーブル、ツイスト・ワイヤ対等の、通信方法で利用可能な任意のものによって、ノード間の通信を確立する。更に、市販のあらゆる形式のパケット交換ネットワーク・ソフトウエアも、ワイド・エリア・ネットワーク１０におけるノード間に通信を確立するために利用することができる。したがって、本発明は、軍環境に制限される訳ではない。

【００１８】図２は、本発明の一実施形態の、特定のタスクを実行するために必要なソフトウエア、ファームウエア、及びハードウエアの一部を示している。図２に示すブロックは、モジュール、コード、コード・セグメント、コマンド、ファームウエア、ハードウエア、並びに、プロセッサを用いたシステム（複数のシステム）によって実行可能な命令及びデータを表している。命令及びデータは、Ｃ＋＋のようなプログラミング言語で書くことができるが、Ｃ＋＋に限定される訳ではない。以下においては、コンピュータのローカル・エリア・ネットワーク又はワイド・エリア・ネットワークにおいて用いられるセキュリティ・システムを対象として説明する。しかしながら、当業者には明らかなように、本発明の実施形態は多数のソフトウエア・アプリケーションにおいても用いることができる。

【００１９】更に図２を参照すると、ローカル・パスワード・ファイル１５００と通信するチャネル・モニタ／フィルタ・モジュール１０００が示されている。チャネル・モニタ／フィルタ・モジュール１０００は、図７に示す動作６５０～ステップ７１０を実行するが、これらに限定される訳ではない。チャネル・モニタ／フィルタ・モジュール１０００は、各ユーザ・ノード、コンピュータ・システム、及び図１に示す軍用車両３０にそれぞれインストールされている。チャネル・モニタ／フィルタ・モジュール１０００は、ワイド・エリア・ネットワーク１０内のブロードキャスト・メッセージ及びマルチキャスト・メッセージを監視し、かつ受信し、コンピュータ・システムの現ユーザが特定のメッセージを視認するために、当該ユーザに必要な特権又はセキュリティ承認（ｃｌｅａｒａｎｃｅ）を判定する機能を有する。チャネル・モニタ／フィルタ・モジュール１０００については、図７を参照して、以降で詳しく論ずることにする。

【００２０】更に図２を参照すると、ユーザ・ログイン・モジュール１２００が設けられており、ユーザのログインを許可し、ユーザの特権及びセキュリティ承認を判定する。ユーザ・ログイン・モジュール１２００は、ユーザにログイン画面を提示し、パスワードの一方向暗号化を行い、ローカル・パスワード・ファイル１５００に記憶されているパスワードと一致するか否かの判定を行なう。ユーザ・ログイン・モジュール１２００は、図３に示したステップ１００～ステップ２００を実行するが、これらに限定される訳ではない。

【００２１】更に図２を参照すると、パスワード管理モジュール１３００が設けられており、該モジュールは、ワイド・エリア・ネットワーク１０内に配置されている全てのローカル・パスワード・ファイル１５００の更新を可能にする。システム管理者のコンピュータ・システム又はセキュリティ担当者のコンピュータ・システムを含む、ワイド・エリア・ネットワーク１０内のあらゆるコンピュータ・システムは、同一のパスワード・ファイルを含んでいる。なお、システム管理者又はセキュリティ担当者のコンピュータ・システムの場合、パスワード・ファイルを、マスタ・パスワード・ファイル１８００と呼ぶことにする。パスワード管理モジュール１３００は、ワイド・エリア・ネットワーク１０内にある全てのコンピュータ・システムが同じパスワード・ファイルを収容することを確実にする。また、パスワード管理モジュール１３００は、オプションとして、パスワード・ファイルの最新版によって更新された、全てのコンピュータ・システムの履歴を維持することも可能である。このパスワード・ファイルは、ワイド・エリア・ネットワーク１０の正規のユーザ全員のユーザＩＤ及びパスワードを全て収容する。また、各ユーザの付随特権も含み、不正者が特権データにアクセスするのを防止する役割も果たす。更に、パスワード・ファイルは、ユーザＩＤだけで構成する必要はなく、正規ユーザのワイド・エリア・ネットワーク１０に対する役割（ｒｏｌｅ）又は肩書き（ｔｉｔｌｅ）に基づいてもよい。また、パスワード・ファイルは、マスタ・パスワード・ファイル１８００及びローカル・パスワード・ファイル１５００双方共、必ずしもユーザの特権を収容する必要はない。何故なら、これらの特権は、別個のファイル内に、パスワード・ファイルからのポインタと共に収容することもできるからである。

【００２２】更に図２を参照すると、リモート監査モジュール１４００が設けられており、ユーザ端末すなわち軍用車両３０上で発生する可能性がある、異常事態又はセキュリティ上重大な事態を監視し処理する。これらの重大な事態は、以下の事項を含むが、これらに限定される訳ではない。
１．ユーザの試行が許容ログイン試行失敗回数を超過した。
２．ユーザに変更が生じたため、セキュリティ承認又は役割を知る必要性が生じた。
３．ユーザによって、システム・ディスエーブル動作が開始された。
４．ユーザのパスワード有効期限が切れた。
５．無効なデジタル署名のために、メッセージが拒絶された。
６．リモート・ユーザの再許可要求がセキュリティ担当者（ＳＯ）によって開始され、リモート・ユーザ端末上で実行された。
７．リモート・ユーザのロックアウト要求がＳＯによって開始され、リモート・ユーザ端末上で実行された。
８．リモート端末のディスエーブル要求がＳＯによって発せられ、リモート・ユーザ端末において開始された。
９．パスワードの遠方入力要求がＳＯによって発せられ、リモート・ユーザ端末上で無事に完了した。
【００２３】上記の異常事態及びその他の異常事態が生じた場合、ユーザのコンピュータ・システムを直ちに停止し、パスワード・ファイル等の重要なファイルを消去することも可能である。あるいは、リモート・コントロール・モジュール１６００を動作させて、システム管理者又はセキュリティ担当者が適切な処置を取るようにすることも可能である。図２のリモート・コントロール・モジュール１６００は、システム管理者又は、セキュリティ担当者が、ある事態が発生した場合に、適切な処置を取ることができるようにしている。上記の事態に応答して処置を講ずることに加えて、システム管理者又はセキュリティ担当者は、単に周期的に又はランダムに、軍用車両３０内にあるユーザ端末上でユーザの再認証を要求することもできる。
【００２４】更に図２を参照すると、認証モジュール１７００が設けられており、ユーザによるローカルな再認証が成功した場合に、（システム管理者又はセキュリティ担当者に対するオプションとして）システム管理者又はセキュリティ担当者のコンピュータ・システムに格納されているマスタ・パスワード・ファイル１８００と突き合せて再認証をチェックし、確認する。ユーザのコンピュータ・システム又は軍用車両３０に格納されているローカル・パスワード・ファイル１５００を、システム管理者又はセキュリティ担当者のコンピュータ・システムに格納されているマスタ・パスワード・ファイル１８００と同一にする必要があるため、認証モジュール１７００は、ユーザの同一性の確認をファイル１５００に返送する。このとき、ローカル・パスワード・ファイル１５００がバイパスされた場合（同一性の確認が返送されなかった場合）に、これを検出し、更にシステム管理者又はセキュリティ担当者によって直ちに適切なリモート・コントロール処置を取るようにする。
【００２５】図3は、本発明の実施形態の一例において用いられるユーザ・ログイン・モジュール１２００において実行される処理のフローチャートである。ユーザ・ログイン・モジュール１２００は、ステップ１００において実行を開始し、その後直ちにステップ１１０に進む。ステップ１１０において、ユーザ／役割ログイン画面をユーザ端末、コンピュータ・システム又は軍用車両３０に提示する。ステップ１２０において、ユーザは彼のユーザＩＤ／役割及びパスワードを入力する。その後、ステップ１３０において、ユーザ・パスワードを一方向暗号化する。一方向暗号化は、Ｓｔａｌｌｉｎｇｓ，Ｗｉｌｌｉａｍの”Ｎｅｔｗｏｒｋ　ｓｅｃｕｒｉｔｙ　ｅｓｓｅｎｔｉａｌｓ：ａｐｐｌｉｃａｔｉｏｎｓ　ａｎｄ　ｓｔａｎｄａｒｄｓ　ｏｎ”（ネットワーク・セキュリティの本質：その応用及び標準）、Ｐｒｅｎｔｉｃｅ－Ｈａｌｌ，ＩＳＢＮ０－１３－０１６０９３－８、２８２～２８５ページに論じられており、その内容はこの言及により本願にも含まれるものとする。ステップ１４０において、ユーザＩＤ／役割、及びステップ１３０において受け取った暗号化パスワードを用いて、ローカル・パスワード・ファイル１５００にアクセスする。ローカル・パスワード・ファイル１５００内のパスワードも一方向暗号化されている。
【００２６】したがって、一致が見出された場合、これは、一方向暗号化パスワードの、格納されている一方向暗号化パスワードとの比較に基づいている。このように、ローカル・パスワード・ファイル１５００が万一不正者の手に落ちても、元のパスワードを解読することはできない。動作１５０において一致が見出された場合、処理はステップ１６０に進む。ステップ１６０において、ユーザのＩＤ／役割特権にアクセスする。これらの特権及びセキュリティ承認を、ユーザＩＤ及びパスワードと関連するビット・パターンとして、ローカル・パスワード・ファイル１５００又は別個に他のファイル内に格納することができる。いずれの場合でも、処理はステップ１７０に進み、ここで、読み出した特権に基づいて、このセキュリティ承認又は特権に関連するメッセージ・セット、ファイル・セット及びソフトウエアにアクセスする。その後、ステップ１８０において、ユーザ・ログイン・モジュール１２００に関する処理を終了する。
【００２７】しかしながら、ステップ１５０において一致が見出されなかった場合、処理はステップ１９０に進み、これがログオンにおける３回目の試行失敗であるか

否か判定を行なう。３回目の試行失敗ではない場合、処理はステップ１１０に戻り、そのユーザに再度ログインするように要求する。しかしながら、これがログオンにおける３回目の試行失敗である場合、処理はステップ２００に進み、リモート監査モジュール１４００の動作を実行する。

【００２８】図４は、本発明の実施形態の一例において用いられるパスワード管理モジュール１３００の動作のフローチャートである。パスワード管理モジュール１３００は、ステップ２５０において実行を開始し、直ちにステップ２６０に進む。ステップ２６０において、ＳＡ／ＳＯ（システム管理者／セキュリティ担当者）は、自身のパスフレーズを入力し、自身の秘密キーの解読／復元を行なう。ステップ２７０において、ＳＡ／ＳＯは、解読した秘密キーを用いて、マスタ・パスワード・ファイルを含むメッセージにデジタル署名し、ワイド・エリア・ネットワーク１０の全てのユーザにブロードキャストする。ステップ２９０において、ワイド・エリア・ネットワーク１０全域にメッセージをブロードキャスト又はマルチキャストするか、又はワイド・エリア・ネットワーク１０上の目標ユーザ又は軍用車両３０にブロードキャスト又はマルチキャストする。ステップ３００において、目標ノード、ユーザ、コンピュータ・システム、又は軍用車両３０は、それらのシステム上にローカルに格納されているＳＡ／ＳＯの公開キーを用いて、デジタル署名を認証する。ステップ３１０において、デジタル署名が認証されたか否か判定を行なう。

【００２９】ステップ３１０においてデジタル署名が認証された場合、処理はステップ３２０に進む。ステップ３２０において、マスタ・パスワード・ファイル１８００を、ローカル・パスワード・ファイル１５００として、ローカル・システム内にインストールする。その後、ステップ３３０において、インストールが成功したか否か判定を行なう。インストールが成功した場合、処理はステップ３４０に進み、パスワード管理モジュール１０００は動作を終了する。しかしながら、ステップ３１０においてデジタル署名が認証されず、ローカル・ユーザ端末がＳＡ／ＳＯに対する適正な公開キーを有していないと判定された場合、又はステップ３３０においてインストールが不成功であったと判定された場合、処理はステップ３５０に進み、リモート監査モジュール１４００が動作する。

【００３０】図５は、本発明の実施形態の一例において用いるリモート・コントロール・モジュール１６００の処理のフローチャートである。リモート・コントロール・モジュール１６００は、ステップ４００において実行を開始し、ステップ４１０において、ＳＡ／ＳＯは、自身のパスフレーズを入力して、自身に関連する秘密キーを解読する。その後、ステップ４２０において、ＳＡ／ＳＯは、忌避（チャレンジ）メッセージにデジタル署名し、ＳＡ／ＳＯ秘密キーを用いて、疑わしいユーザ・ノードに配信する。この忌避は、多数の事態が原因で生じる可能性がある。これらの事態は、ランダムな要求から、敵部隊による軍用車両３０の捕獲容疑に対する再認証まで、任意のものを含むことができる。次いで、ステップ４３０において、忌避を含むメッセージを、軍用車両３０のような目標ユーザ・ノードに送信する。メッセージの受信時に、ステップ４４０において、目標ノードはＳＡ／ＳＯ公開キーを用いて署名を認証する。ステップ４５０において、ＳＡ／ＳＯの公開キーを用いて、メッセージが認証されたか否か判定を行なう。メッセージが認証されなかった場合、処理はステップ４５５に進み、リモート監査モジュール１４００が動作する。ステップ４５０におけるデジタル署名の認証失敗は、不正ユーザがＳＡ／ＳＯになりすまそうとしたことを示す可能性がある。そして、ステップ５４５において、リモート・コントロール・モジュール１６００は処理を終了する。

【００３１】しかしながら、ＳＡ／ＳＯのデジタル署名がステップ４５０において認証された場合、処理はステップ４６０に進む。ステップ４６０において、ユーザ／役割ログイン画面がユーザ端末に表示される。ユーザ端末を、軍用車両３０内に配置することもできる。その後、処理はステップ４７０に進み、時間切れとなってユーザがパスワードを入力し損ねたか否か判定を行なう。時間切れになっていない場合、処理はステップ４９０に進み、ユーザが入力したパスワードが正しいか否か判定する。ステップ４７０において、時間切れ状態であると判定した場合、又はステップ４９０において、パスワードが正しくないと判定した場合、処理はステップ４８０に進む。ステップ４８０において、今回の試行がユーザによる正しいパスワードを入力しようとし損ねた３回目の試行であるか否かの判定を行なう。ステップ４８０において、これが３回目の試行失敗でないと判定した場合、処理はステップ４６０に戻り、ユーザに再度正しいパスワードを入力するように要求する。ログインの試行失敗を３回に限らず、任意の回数に設定可能であり、完全にＳＡ／ＳＯの自由に決められる。

【００３２】一方、ステップ４８０において、これがユーザによる３回目のログイン試行の失敗であると判定した場合、処理はステップ５１０に進み、リモート監査モジュール１４００を実行する。その後、処理はステップ５２０に進み、ＳＡ／ＳＯは軍用車両３０内に配置することができるユーザ端末に対する制御レベルを高める。ＳＡ／ＳＯは、ステップ５３０、５３５、５４０において示すように、少なくとも３つの使用可能な選択肢を有する。しかしながら、これらは、例示のために限定した選択肢の数であり、可能性の全てを網羅したのではない。ステップ５３０において、ＳＡ／ＳＯは、軍用車両３０内に配置することができる端末画面をロックし、ユ

ーザは、自身のユーザＩＤ及びパスワードを再認証するために、ログイン画面に応答することのみが可能となるようにする。その後、処理はステップ５３０からステップ４２０に進み、ユーザは忌避メッセージを受信し、再度ステップ４６０において正しいパスワードを入力することができる。このとき、ステップ４６０においては、ユーザに対して、画面ロック状態が存在して他の機能は許されていないことの指示も提供される。

【００３３】更に、ＳＡ／ＳＯは、ステップ５３５において、軍用車両３０内に配置されるユーザ端末を完全にディスエーブルすることもできる。ユーザ端末を完全にディスエーブルするには、ユーザ・ディスク・ドライブ又はメモリ上の所定のファイルを削除し、システムを停止することを含んでいる。ステップ５４０では、ＳＡ／ＳＯは、システム及びワイド・エリア・ネットワーク１０へのログインに成功したと信じさせるように、ユーザを欺くことを決定することができる。ステップ５４０において、ＳＡ／ＳＯは、ユーザを欺くために、偽情報をユーザに供給することができ、これは無期限に続けてもよい。ステップ５３５を選択した場合、処理はステップ５４５に進み、リモート・コントロール・モジュール１６００の処理は終了する。

【００３４】図６は、本発明の実施形態の一例において用いるリモート監査モジュール１４００の処理のフローチャートである。リモート監査モジュール１４００は、ステップ５５０において実行を開始し、ステップ５６０において、軍用車両３０内にあるローカル・ユーザ端末によって、異常事態が検出される。発生し得る異常事態の種類は、既に論じたので、ここでは繰り返さない。その後、ステップ５７０において、この異常事態をＳＡ／ＳＯに報告する。次いで、ステップ５８０において、ユーザ端末を直ちに停止すなわちシャットダウンするか否か判定を行なう。この即時停止を行なうのは、車両が正に捕獲されようとしていると兵士が判断し、端末上でその旨を兵士が指示したときである。ユーザ端末を直ちに停止すべき場合、ステップ５９０において、切迫停止の報告がＳＡ／ＳＯに送られる。ステップ６００において、選択された重要ファイルを消去する。最後にステップ６１０において、ユーザ端末を停止すなわちシャットダウンする。その後、処理はステップ６２０に進み、リモート監査モジュール１４００は処理を終了する。一方、ステップ５８０において、即時停止が必要でないと判定した場合、処理はステップ６３０に進み、リモート・コントロール・モジュール１６００の機能を実行する。

【００３５】図７は、本発明の実施形態の一例において用いるチャネル・モニタ／フィルタ・モジュール１０００の処理のフローチャートである。チャネル・モニタ／フィルタ・モジュール１０００はステップ６５０において実行を開始し、ステップ６６０において、軍用車両６６０内のユーザ端末がメッセージを受信する。ステップ６７０において、ユーザ端末はメッセージの発信元を特定する。その後、ステップ６８０において、ユーザ端末はローカル・パスワード・ファイル１５００にアクセスし、ユーザ端末に現在ログインしているユーザの特権を読み出す。その後、ステップ６９０において、現ユーザが、アクセス可能でありかつステップ６６０において受信したメッセージを見ることができるか否かの判定を行なう。ステップ６９０において、現ユーザがステップ６６０において受信したメッセージを見ることができると判定した場合、処理はステップ７１０に進み、ユーザにメッセージを表示する。その後、ユーザがメッセージを見たか否かには係らず、処理はステップ７００に進み、チャネル・モニタ／フィルタ・モジュール１０００の処理を終了する。

【００３６】図８は、本発明の実施形態の一例において用いる認証モジュール１７００の処理のフローチャートである。認証モジュール１７００は、ステップ７４０において実行を開始し、ステップ７５０において、ユーザ端末、すなわち軍用車両３０は、メッセージにデジタル署名し、ユーザが署名認証データと共に入力したユーザ・パスワードを、ＳＡ／ＳＯ公開キーを用いて暗号化する。このＳＡ／ＳＯ公開キーは、元々ユーザ端末にインストールされていたか、ＳＡ／ＳＯによって後日ダウンロードされたものである。次に、ステップ７６０において、ユーザ端末はメッセージをＳＡ／ＳＯに送る。次いでステップ７７０において、ＳＡ／ＳＯは、メッセージ受信時に、直ちに署名を認証し、自身のパスフレーズを入力した後に、自身の公開キーを用いて、署名認証データと共にユーザ・パスワードを解読する。受信した暗号化キーを解読することができれば、ユーザが適切な公開キーを有していることの証明となる。その後、ステップ７８０において、パスワードを一方向暗号化し、ステップ７９０において、マスタ・パスワード・ファイル１８００にアクセスする。ステップ８００において、マスタ・パスワード・ファイル１８００に一致が見出された場合、ユーザは正規のユーザであると判定し、処理はステップ８３０に進み、認証モジュール１７００は処理を終了する。

【００３７】一方、ステップ８００において、一致していないと判定された場合、軍用車両３０内のユーザ端末のローカル・パスワード・ファイル１５００は損なわれていると仮定することができる。この仮定は、処理中にこの点に到達するためには、ユーザが、軍用車両３０内のユーザ端末上で、ローカル・パスワード・ファイル１５００に格納されているパスワードを入力する必要があったからであると結論づけることができる。ステップ８１０において、リモート監査モジュール１４００の実行によって、パスワード・ファイルの障害可能性をＳＡ／ＳＯに警告する。その後、ステップ８２０において、Ｓ

Ａ／ＳＯは、適切と考えられるあらゆる処置を講ずることができる。この処置には、ユーザのコンピュータ・システムをディスエーブルすること、又は先に論じたような妨害動作を実行することを含ませることができる。

【００３８】本発明の実施形態を用いると、システム管理者又はセキュリティ担当者は、オーバーヘッド及びネットワーク上の通信における干渉を最少限に抑えて、ローカル・エリア・ネットワーク又はワイド・エリア・ネットワーク上におけるセキュリティを管理することができる。これは、各ユーザ・コンピュータ上に常駐し、誰にも解読が不可能な一方向暗号化パスワードを格納するパスワード・ファイルを使用することによって達成される。この一方向暗号化パスワードを格納するファイルによって、ユーザはネットワーク内のあらゆるシステムにもログオンすることができ、自身のセキュリティ・レベル及び特権に対して許可されているソフトウエア及び情報にアクセスすることができる。しかしながら、ローカル・パスワード・ファイルを迂回しても、本発明の一実施形態ではこれを検出し、システム管理者又はセキュリティ担当者は適切な処置を講ずることができる。更に、本発明の実施形態を実現するために必要な一連の処理は、ユーザ・コンピュータ・システム上で行われ、ネットワークの動作に対する影響は最少で済む。尚、全てのパスワードは一方向暗号化されており、全ての秘密キーはパスフレーズを用いて暗号化されているので、不正ユーザがこれらにアクセスするのは困難である。したがって、パスワードも秘密キーも明文で格納されていないので、不正ユーザはアクセスすることはできない。

【００３９】以上いくつかの例のみについて示しかつ説明したが、当業者にはわかるように、本発明には多数の変更や修正も可能である。例えば、無線及びマイクロ波通信の使用に言及したが、本発明は、これらの通信形態に限定される訳ではない。本発明の実施形態は、公衆電話交換網上のツイスト・ワイヤ対からリース回線まで、更に同軸及び光ファイバ・ケーブル等あらゆるものを用いたあらゆる種類のローカル・エリア・ネットワーク又はワイド・エリア・ネットワークにおいても動作可能である。更に、ネットワークにおける通信には、任意の種類の通信ソフトウエアを使用可能である。したがって、ここに示しかつ記載した詳細に限定されることなく、かかる変更及び修正は全て、添付の特許請求の範囲によって包含されるものである。

【図面の簡単な説明】

【図１】軍環境において実現したワイド・エリア・ネットワークの一例を示す図である。

【図２】本発明の一実施形態において用いられるソフトウエア、ファームウエア、及びハードウエアのモジュール構成図である。

【図３】本発明の一実施形態において用いられるユーザ・ログイン・モジュールの処理のフローチャートである。

【図４】本発明の一実施形態において用いられるパスワード管理モジュールの処理のフローチャートである。

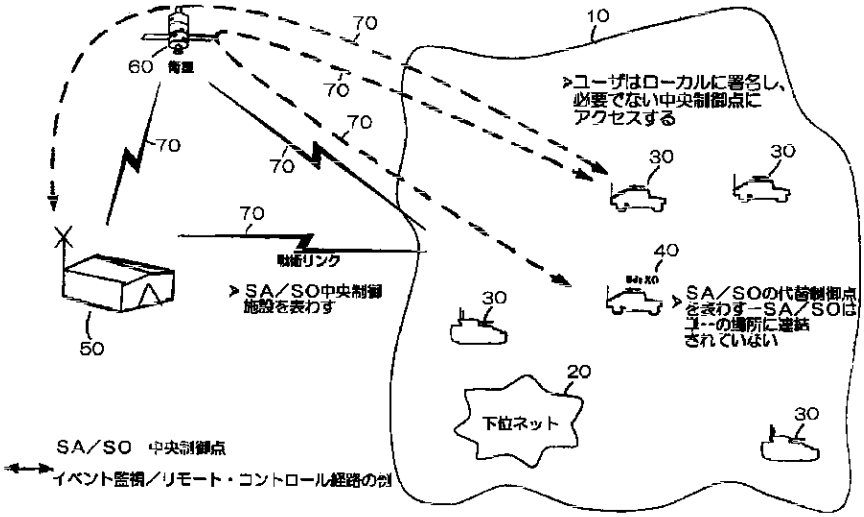
【図５】本発明の一実施形態において用いられるリモート・コントロール・モジュールの処理のフローチャートである。

【図６】本発明の一実施形態において用いられるリモート監査モジュールの処理のフローチャートである。

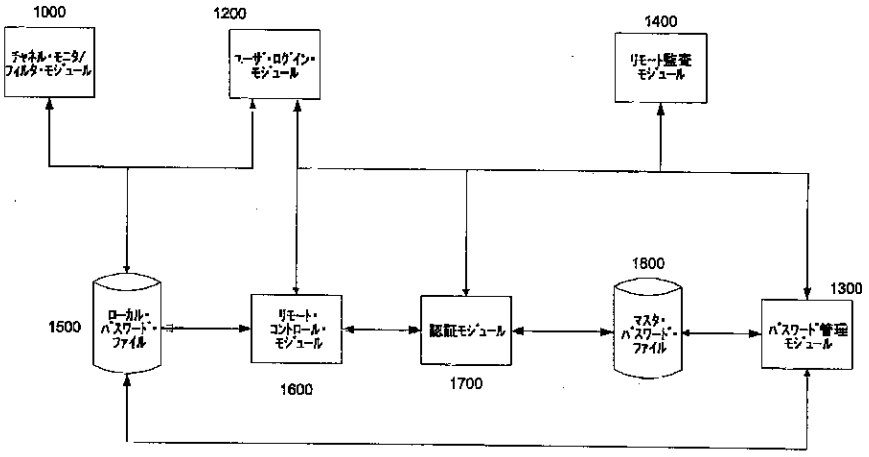
【図７】本発明の一実施形態において用いられるチャネル・モニタ／フィルタ・モジュールの処理のフローチャートである。

【図８】本発明の一実施形態において用いられる認証モジュールの処理のフローチャートである。

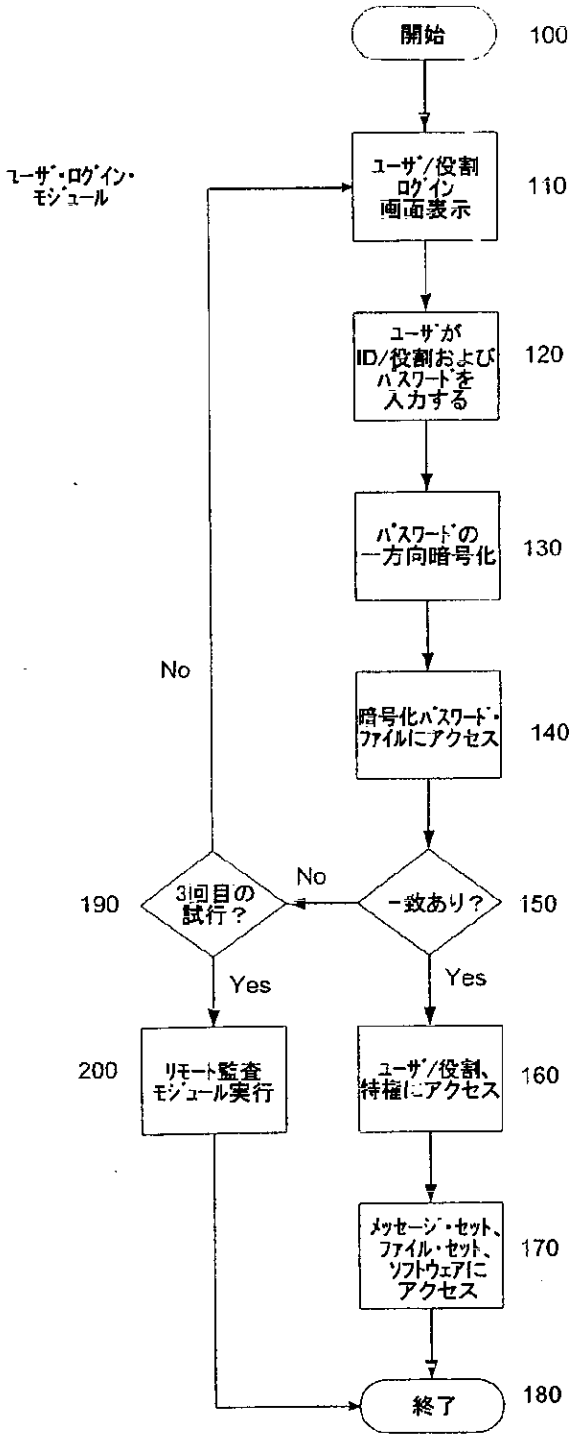
【図１】



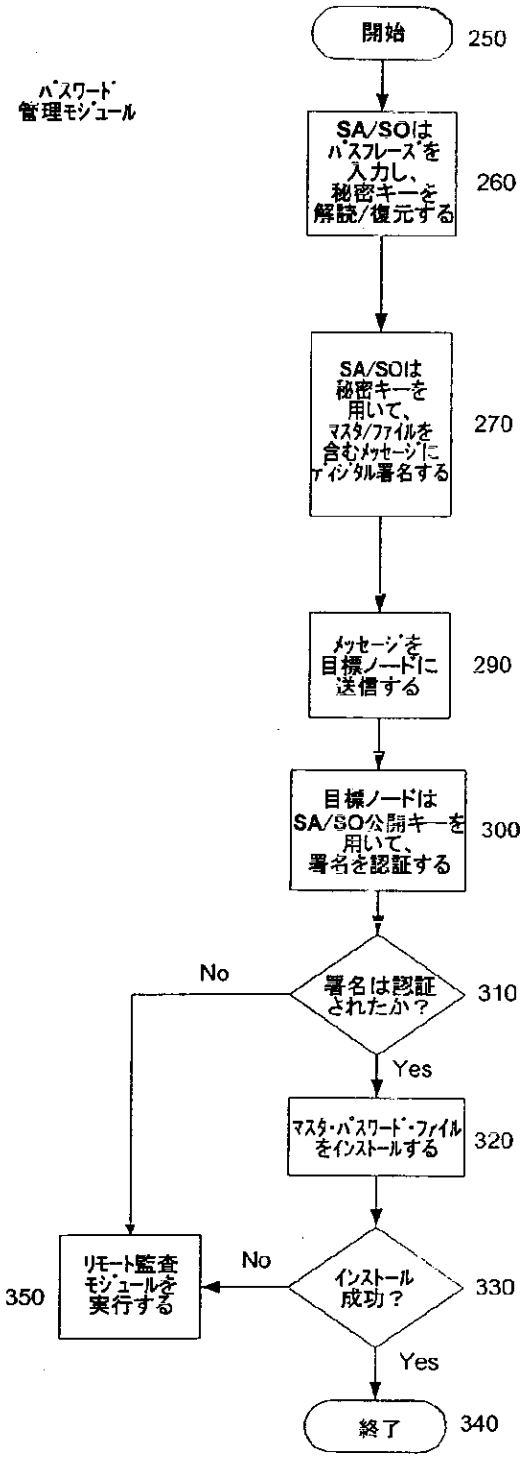
【図2】


1000
チャネル・モニタ/フィルタ・モジュール
1200
ユーザ・ログイン・モジュール
1400
リモート監査モジュール
1500
ローカル・パスワード・ファイル
リモート・コントロール・モジュール
1600
認証モジュール
1700
1800
マスタ・パスワード・ファイル
1300
パスワード管理モジュール

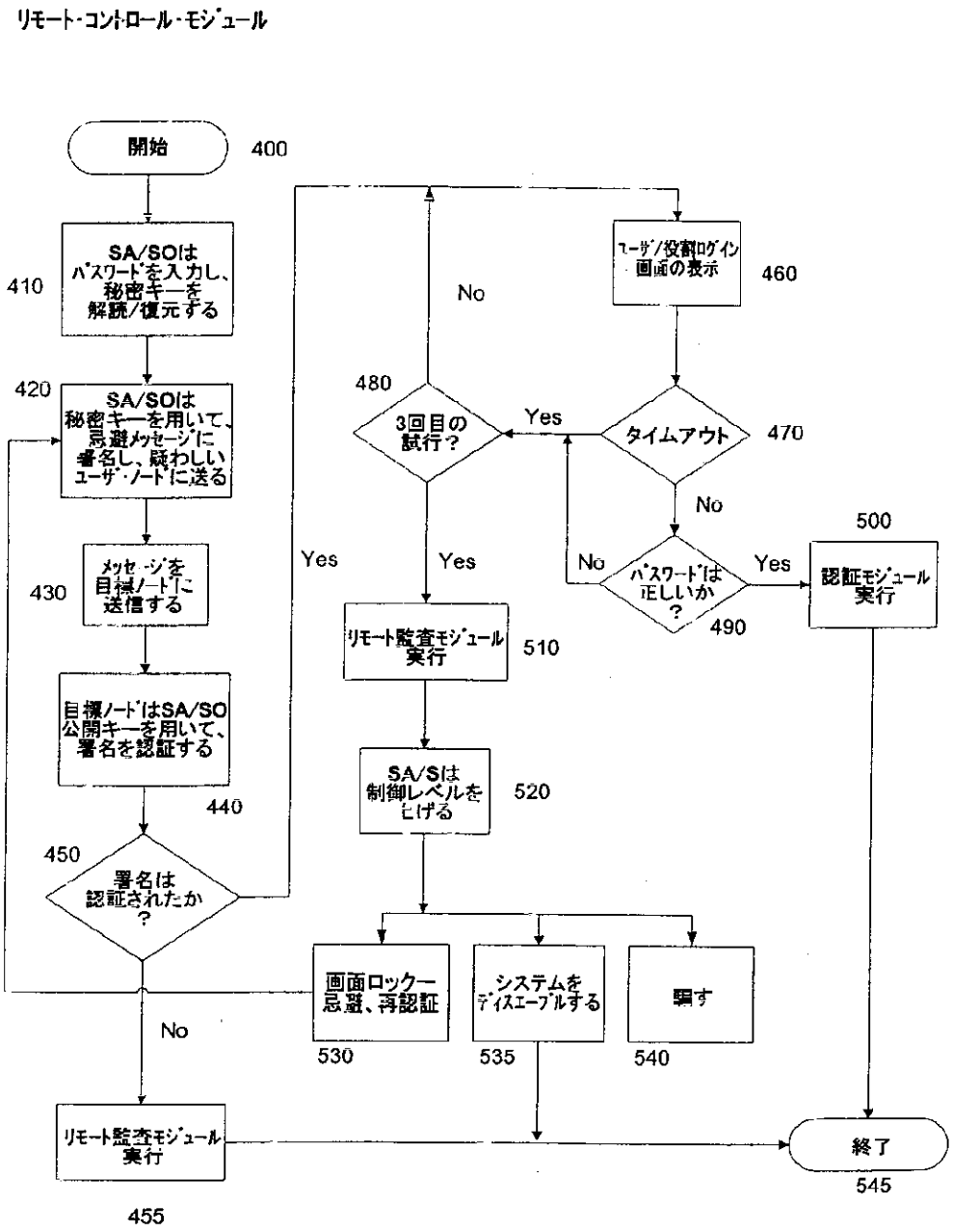
【図3】


開始
100
ユーザ・ログイン・モジュール
ユーザ/役割ログイン画面表示
110
ユーザがID/役割およびパスワードを入力する
120
パスワードの一方向暗号化
130
暗号化パスワード・ファイルにアクセス
140
一致あり？
150
No
3回目の試行？
190
No
Yes
Yes
リモート監査モジュール実行
200
ユーザ/役割、特権にアクセス
160
メッセージ・セット、ファイル・セット、ソフトウェアにアクセス
170
終了
180

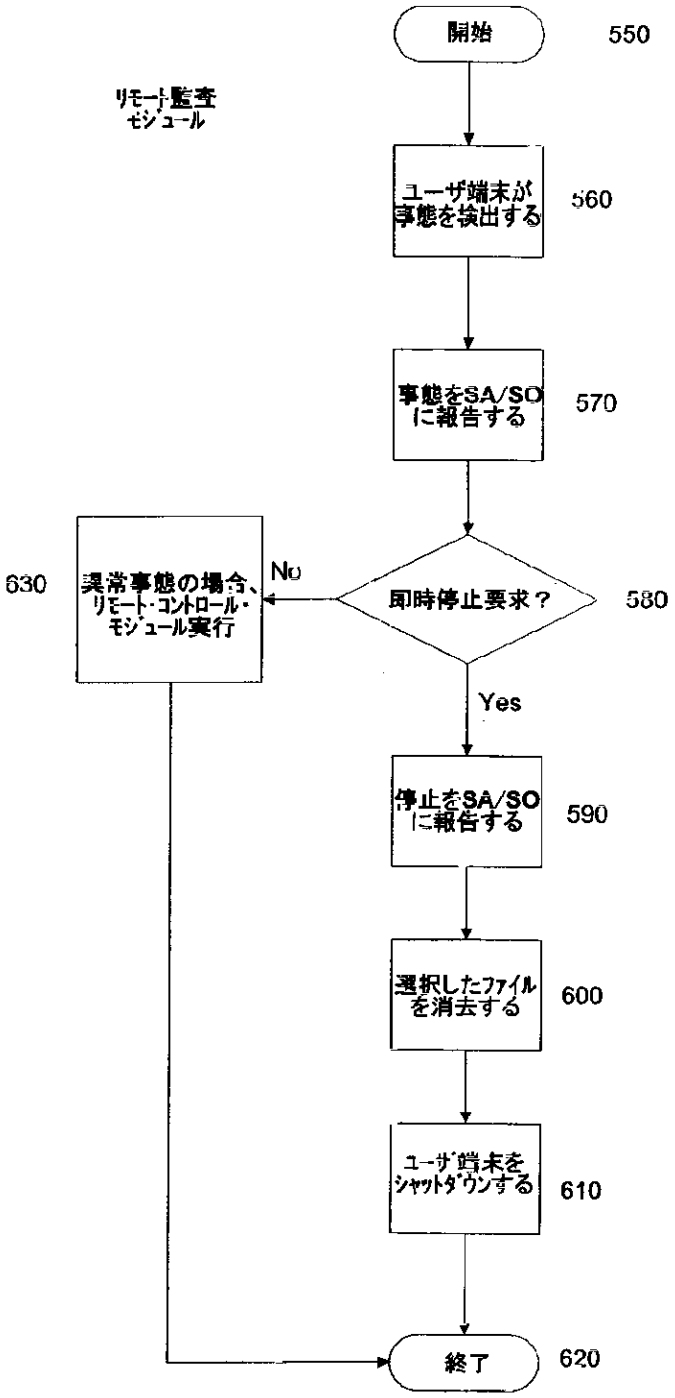
【図4】


開始
250
パスワード管理モジュール
SA/SOはパスフレーズを入力し、秘密キーを解読/復元する
260
SA/SOは秘密キーを用いて、マスタ/ファイルを含むメッセージにディジタル署名する
270
メッセージを目標ノードに送信する
290
目標ノードはSA/SO公開キーを用いて、署名を認証する
300
署名は認証されたか？
310
No
Yes
マスタ・パスワード・ファイルをインストールする
320
インストール成功？
330
No
Yes
リモート監査モジュールを実行する
350
終了
340

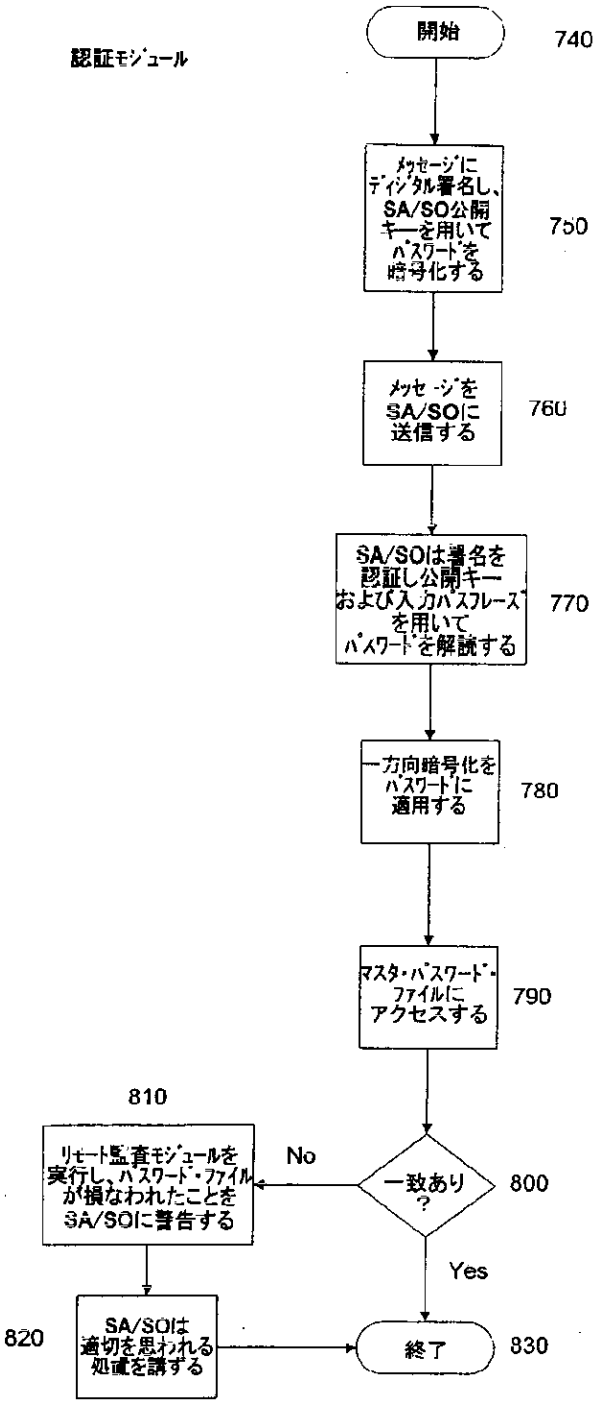
【図5】


リモート・コントロール・モジュール
開始
400
SA/SOは パスワードを入力し、秘密キーを解読/復元する
410
SA/SOは 秘密キーを用いて、忌避メッセージに署名し、疑わしいユーザ・ノードに送る
420
メッセージを目標ノードに送信する
430
目標ノードはSA/SO公開キーを用いて、署名を認証する
440
署名は認証されたか？
450
Yes
No
リモート監査モジュール実行
455
ユーザ/役割ログイン画面の表示
460
タイムアウト
470
パスワードは正しいか？
490
No
Yes
認証モジュール実行
500
3回目の試行？
480
No
Yes
リモート監査モジュール実行
510
SA/Sは 制御レベルを上げる
520
画面ロック−忌避、再認証
530
システムをディスエーブルする
535
騙す
540
終了
545

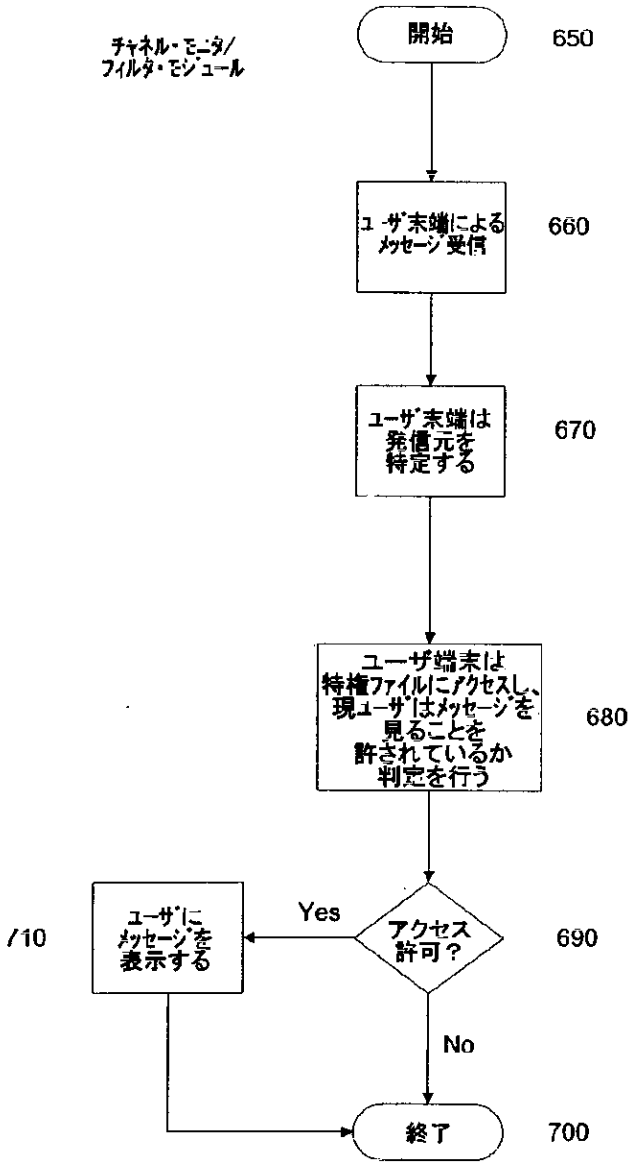
【図6】


リモート監査モジュール
開始
550
ユーザ端末が事態を検出する
560
事態をSA/SOに報告する
570
即時停止要求？
580
No
異常事態の場合、リモート・コントロール・モジュール実行
630
Yes
停止をSA/SOに報告する
590
選択したファイルを消去する
600
ユーザ端末をシャットダウンする
610
終了
620

【図8】


認証モジュール
開始
740
メッセージにディジタル署名し、SA/SO公開キーを用いてパスワードを暗号化する
750
メッセージをSA/SOに送信する
760
SA/SOは署名を認証し公開キーおよび入力パスフレーズを用いてパスワードを解読する
770
一方向暗号化をパスワードに適用する
780
マスタ・パスワード・ファイルにアクセスする
790
一致あり？
800
No
リモート監査モジュールを実行し、パスワード・ファイルが損なわれたことをSA/SOに警告する
810
SA/SOは適切と思われる処置を講ずる
820
Yes
終了
830

【図7】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
H04L 9/32		H04L 9/00	673C

(72)発明者 ロナルド・ジェイ・コゼル
アメリカ合衆国カリフォルニア州，リダンド・ビーチ

(72)発明者 デイヴィッド・シー・ビクスラー
アメリカ合衆国カリフォルニア州，ハーモサ・ビーチ

Fターム(参考) 5B017 AA03 BA05 BA07 CA15 CA16
5B082 EA12
5B085 AE02 AE03 AE09 BC01
5J104 AA07 KA01 KA03 NA05 PA07