<table>
<thead>
<tr>
<th>項目</th>
<th>内容</th>
</tr>
</thead>
<tbody>
<tr>
<td>特許出願公開番号</td>
<td>特開2002－63140 (P2002－63140A)</td>
</tr>
<tr>
<td>開示日</td>
<td>平成14年2月28日 (2002.2.28)</td>
</tr>
</tbody>
</table>

件名：ネットワーク上のアクセス管理方法及びシステム

要約：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、一方向性化パスワード、及び権限を記憶する。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。チャンネル・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、ユーザの権限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。リモート監視モジュール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名関係に関する、複数のユーザ識別（ID）と、複数の方向暗号化パワードと、複数の付随特権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１D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１D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ェ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通信されるソフトウェア、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１D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１D及び一方向暗号化された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１D及び一方向暗号化パスワードを少なくとも1個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１D及び一方向暗号化パスワードに一致するユーザ１D及び一方向暗号化パスワードをユーザが提示できる旨の通知を通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１D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と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、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、ユーザを飲んで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、飲くステップは、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プルし、ユーザが該コンピュータ・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からコンピュータにおいて異常事態が検出されるステップと、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えたこと、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・ディスエプ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・ユーザの締め出しが求が、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プ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、又はユーザを散るか、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仮名化パスワード・ファイルにおいて、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、関連する一方仮名化パスワード、及び仮名化特権を含んでいる、一方仮名化パスワード・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、一方仮名化パスワード・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プ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つつ送信し、ユーザの仮名化特権がメッセージの認識を許可する場合、メッセージをユーザに表示する、ネットワーク・セキュリティ・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、同じ一方仮名化パスワード・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を許容可能な失敗回数を超えたこと、ユーザの仮名化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側軸を切られたこと、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・ユーザの縮み出し要求が、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・ローキング・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させるリモート・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要求されたときに、乗算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・ファイルに組み合せてチェックすることによって、ユーザID・ログイン・モジュール及びコンピュータ内に収容されている一方仮名化パスワードにおいて一致を検出した後、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、一方仮名化パスワード、及び仮名化特権を含むマスタ・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使用してメッセージを仮名化し、該メッセージを全てユーザにプ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仮名化パスワード・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、一方仮名化パスワード、及び仮名化特権を含んでいる一方仮名化パスワード・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、一方仮名化パスワード・ファイル中にこれ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ID・ログイン・コード・セグメントと、ネットワーク内においてプロードキャスト・メッセージを監視しつつ送信し、
ユーザの付随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・モンタゴルフ・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、該プログラムはさらに、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・ファイルを取得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、該プログラムはさらに、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・ディスエープ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・ユーザの総合し出し要求が、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・ローキング・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、該プログラムはさらに、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、該プログラムはさらに、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・ファイルに突き合わせてチェックすることによって、ユーザ・ログライン・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、セキュリティ及び生存力（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。更に特徴すれば、本発明は、アクセス及び制御に関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量された契約番号DAAB07-95-D-064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 通常の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、ハードウェア価格の低下が急速な導入、及びコンピュータ・ハードウェアの性能、信頼性、サイズ及び堅固性に関する著しい改善である。コンピュータの信頼性及び性能は、軍用コンピュータを個々の戦車車両・戦車・戦車用に使用可能なことにより向上している。このようなコンピュータのマイ・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ェア・サイズ（Sheer size）が小さい。様々なタイプのコンピュータの数多く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、ユーザのシーケンス、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ない場合もある。更に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式のみ、直接的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、ネットワーク上のデータ伝送速度に限界がある。高速ケーブルを使用したネットワーク利用の場合でも、ネットワーク上のノード数が拡大するために、管理用データ・トラフィックを絶対的な最少数に制限することは、避けられない。

【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とアクセスする兵歩の водо、ネットワークを通じて伝達される情報の内容が、再認識を求め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。
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ないし、しかも管理するにはかなりのメン・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動きを傍受することが可能になると、戦闘において敵に圧倒的に有利に進まってしまう。

【0005】大きなワード・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ード・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単兵と同じカテゴリーに該当する。即ち、従業員がワード・エリア・ネットワーク上の情報全にアクセスする必要性はなく、その要求もない。更に、従業員は、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るから、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、権限のある人材に必要な情報を無視して容易にアクセスさせることができ、一方、不正者を阻止することとは、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、出没するハッカーが含まれる。最近における国内コンピュータのサービス業の試みや、電子メール・ビール・スノーサイド・内部ドームの一部が一いつ発でノート書にされ、様々な無駄や貴重な情報の損失のために、何十億ドルもの費用が、ハッカーによって発生する可能性がある。更に、ハッカーは、不正に持ち出され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ビス上には一上のパスワード・フィアというものが存在しており、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、サーバ内のそれに照合される。これは、潜在的な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上で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ルネックすなわち限界となる。更に、アクセスを得る際には、ユーザが常にネットワーク上の単一のサーバーにログインしなければならないため、ユーザ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、ネットワーク全体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、クリティカル・システムならずとも暗号化されていないグローケーワークを通じてサーバーに転送されており、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、サーバー上では単にサーバーを保持する場合もあるが、この場合、サークルは、従来の戦争、ならびに軍及び役務企業双方に適用可能なサイバー戦争にとって、戦場における目的となる。

【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、新たに割り当てられたコンピュータ・システムにログインし、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は許可されない。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、従業員は別のコンピュータを用いて、新た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。

【0100】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な通信トрафикは絶対的な最少生に止めつつ、ローカル・エリア・ネットワーク及びワード・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、及び適正セキュリティ許可がユーザに対して、アクセスを制限させることのないように、また、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可能になる。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ーに対する完全なアクセスが可能であるも、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ぐようにしなければならない。また、セキュリティが確立され、システム上の不正アクセスを防止するためには、システム上の不正アクセスを防止しなければならない。
【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で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。この方法は、開発したネットワーク内のコンピュータに、一方ルート管理者を含むローカル・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、ネットワーク上の各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ユーザに、数値のユーザ識別ID（ID）、一方ルートパスワード、及び付加特権を含んでいる。ユーザが入力した一方ルートパスワードは、パスワード・ファイル内に格納されている一方ルートパスワードと一致してチェックされる。一方ルート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で収容されているデータ及びソフトウェア内、ユーザの付加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。一方ルート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、付加特権によって許可されるメッセージをユーザに表示する。

【0014】更に、本発明の一実施形態は、数値のコンピュータを有するネットワーク上で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、一方ルート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が許可されている正規のユーザに、数値のユーザID、接続する（一方ルートパスワード）及び付加特権を含んでいる。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、一方ルート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、このシステムは、チャンネル・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、ユーザの付加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。

【0015】更に、本発明の一実施形態は、コンピュータによる実行の可能性があり、コンピュータ読み取り可能媒体上に記憶され、数値のコンピュータを有するネットワーク上でネットワークを有するユーザID又は役割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、一方ルートパスワードを含むパスワード・ファイルを有する。一方ルートパスワード・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ユーザ毎に、数値のユーザID、関連する（一方ルートパスワード、及び付加特権を含む。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、及びパスワードを受信し、一方ルート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、チャンネル・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プロードキャスト・メッセージはマルチキャスト・メッセージを監視し、ユーザの付加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。
なわちシステム管理者又はセキュリティ担当者（SA/SH）車両内に配置している。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SH内に装備される任意のユーザ端末に配置できる。しかし、SA/SH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体SH内に配置されることも通常である。構体SH内及びワード・エリア・ネットワーク100間の通信は、無線周波数信号700を通して、直接的に又は衛星600を経由して行われる。更に、ワード・エリア・ネットワーク100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に示すワード・エリア・ネットワーク100は、作戦環境における軍用に応じた無線通信用を限定することが望ましい。ワード・エリア・ネットワーク20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ード・エリア・ネットワークがなければ、同軸ケーブル、光ファイバケーブル、ワイヤ・スイッチ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、市販の利用する従来のネットワーク・ソフトウェアも、ワード・エリア・ネットワーク100におけるノード間の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、軍環境で制限される訳ではない。

【0018】図2は、本発明の一実施形態の、特定のデータを実行するために必要なソフトウェア、ファームウェア、及びハードウェアの一部を示している。図2に示すブロックは、システム、コード、コード、セグメント、コマンド、ファームウェア、ハードウェア、及びプロセスを用いたシステム（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ード・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、当業者には明らかのように、本発明の実施形態は多数のソフトウェア・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、ワード・エリア・ネットワーク100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、かつ反応し、コンピュータ・システムの限られたメッセージを確認するために、当該ユーザに必要とされるセキュリティ承認（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、以降で詳しく論述することにする。

【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、ユーザの権限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、パスワードの一方略号化を行い、ローカル・パスワード・ファイル1500に記録されているパスワードを一致するか否かの判定を行う。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、該当モジュールは、ワード・エリア・ネットワーク100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こと。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と呼ぶことにより、パスワード管理モジュール1300は、ワード・エリア・ネットワーク100内にある全てのコンピュータ・システムが同時にパスワード・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、ワード・エリア・ネットワーク100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、各ユーザの付加特権も含み、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、正規ユーザのワード・エリア・ネットワーク100に対する権限（role）又は口述（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車両車両300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問題を監視し判断する。これらの重大な事態は、以下の事項を含むが、これらに限定されず得ない。

1. ユーザの認証が許容ログイン試行失敗回数を超えるため。
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. ユーザパスワード有効期間が切れた。
5. 無効なデジタル署名の検出のために、メッセージが削除された。
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によって発させられ、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によって発させられ、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とることができる。このモジュールは、システム管理者又はセキュリティ担当者が、ある状態が発生した場合に、適切な処置をとることができるようになっている。上記の状態に応じて処置を講じることができる。システム管理者又はセキュリティ担当者は、単に定期的に又はランダムに、車両300に配置された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・システムに接続されているマスタ・パスワード・ファイル1800とリスクして再認証をチェックし、確認する。ユーザのコンピュータ・システム又は車両車両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ィールド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、本発明の実施例の一例において用いるユーザ・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・役割ロジック画面をユーザ端末、コンピュータ・システム又は車両車両30に提示する。ステップ120において、ユーザは使用者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、Stalling's, Williamの“Network security essentials: applications and standards on”（ネットワーク・セキュリティの基本：その応用及び標準）、Prentice-Hall, ISBN60-13-016093-8、282-285ページに論じられており、この内容はこの言及により本願に含まれるものとする。ステップ1400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。このようなローカル・パスワード・ファイル1500が万々一不正者が手に落ちても、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IID/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は個別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ェアにアクセスする。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、これがログインにおける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、これがログインにおける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るパワーソフトウェア管理モジュール1300の動作のフローチャートである。パワーソフトウェア管理モジュール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をデジタル署名し、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上の目標ユーザを軍用車両30にブロードキャストするか、又はローカルシステム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に、ローカルシステム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、パワーソフトウェア管理モジュール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たローカル・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に動作する。

【0030】図4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、自身の秘密キーを解読する。その後、ステップ420において、SA／SOは、仮想ビューセッションにデジタル署名し、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。この疑点は、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、ログインに必要な項目や、敵部隊による軍用車両30の捕獲や盗難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、仮想ビューセッションを軍用車両30の全てのユーザに配信する。メッセージの認証時に、ステップ440において、目標ユーザは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う。メッセージが認証されなかった場合、処理はステップ450に進み、リモート監査モジュール1400に動作する。ステップ450におけるデジタル署名の認証失敗、不正ユーザがSA／SOになるか否かを示す可能性がある。そして、ステップ450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、ユーザノート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に配置することもできる。その後、処理はステップ470に進む。時間切れになってユーザがパスワードを入力しなくなったか否か判定を行う。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、時間切れユーザによる正しいパスワードを入力しようとした場合の試行があるか否かを判定する。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には、処理はステップ490に進み、ユーザが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に配置することの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、例えばために選択肢の数であり、可能性が全てを網羅したものではない。ステップ530において、SA／SOは、軍用車両30に配置することができるユーザ端末画面をロールし、
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420に進み、ユーザは認証メッセージを受信し、再度ステップ640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されていないことを指示する。

【0033】更に、SA/SOは、ステップ535において、軍用車両30において配置されるユーザ端末を完全にディーエルプすることができる。ユーザ端末を完全にディーエルプするには、ユーザ・ディスク・ドライプス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40において、SA/SOは、ユーザを滅すために、偽情報をユーザに提供することができるが、これは無期限に続いてもよい。ステップ360において、機能はステップ45において、リモート・コントロール・モジュール1600の処理が終了する。

【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535において実行を開始し、ステップ560において、軍用車両30においてリモート・ユーザ端末によって、異常状態が検出される。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させるシャットダウンをするか否かを判断する。この命令停止を行うのは、車両が正に捕獲されるようとしている兵士が判断し、端末上でその旨を兵士が指示するときである。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るよう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、即時停止が必要であると判定した場合、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。チャネル・モニタ・フィルター・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・フィルター・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において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、ユーザがアクセス可能であるかステップ660において受信したメッセージを見ることができるように情報の処理を行う。ステップ690において、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、ユーザが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を知らせる。処理はステップ700に進み、チャネル・モニタ・フィルター・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、ユーザ端末を直接にサーバに送信することができる。これにより、ユーザがサーバに直接認証を行うことが可能である。しかし、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、メッセージを受け取ると、自身のパスフレーズを入力した後に、自身の認証キーを用いて、認証モジュールを起動する。このSA/SO認証キーは、元々ユーザ端末にインストールされていたが、SA/SOによって後日ダウンロードされたものである。次いで、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、メッセージを受け取ると、自身のパスフレーズを入力した後に、自身の認証キーを用いて、認証モジュールを起動する。
A/SOは、適切と考えられるあらゆる処置を講ずることできる。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、オーガニック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・レベル及び権限に対して許可されているソフトウェ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・ファイルを回収しても、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限に抑え、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ワード用いて暗号化されているので、不正ユーザがこれ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かに格納されないので、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例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、公衆電話回線網上のツイスト・タイや対からリッジ回線まで、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ェアを使用可能である。したがって、ここに示しきつか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つ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ネットウエア、ファームウエア、及びハードウェ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】
リモート・コントロール・モジュール

開始 400

410 SA/SDはパスワードを入力し、秘密キーを解読/復元する

420 SA/SDは秘密キーを用いて、見通しデータに署名し、戻りデータに送る

430 処理ノードはSA/SDの署名を検査する

440 署名は検査されたか？

450 Yes 455 リモート監査モジュール実行

460 No 440 署名は検査されたか？

480 3項目の検行？

470 No タイムアウト 490 パスワードは正しいか？

490 Yes Yes 510 リモート監査モジュール実行

500 No 520 SA/SDの秘密キーを解読する

530画面ロック解除、再認証

535システムをデスブルする

540 録録

終了 545