(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5598112号
(P5598112)
(45)発行日　平成26年10月1日(2014.10.1)　(24)登録日　平成26年8月22日(2014.8.22)

(51)Int.Cl.　F I
G06Q 50/04 (2012.01)　G06Q 50/04

請求項の数 10　(全 14 頁)

(21)出願番号　特願2010-140656(P2010-140656)
(22)出願日　平成22年6月21日(2010.6.21)
(65)公開番号　特開2011-3197(P2011-3197A)
(43)公開日　平成23年1月6日(2011.1.6)
審査請求日　平成25年5月14日(2013.5.14)
(31)優先権主張番号　1459/CHE/2009
(32)優先日　平成21年6月22日(2009.6.22)
(33)優先権主張国　インド(IN)

(73)特許権者　000006507
横河電機株式会社
東京都武蔵野市中町２丁目９番３２号
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100108578
弁理士　高橋　詔男
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100094400
弁理士　鈴木　三義
(74)代理人　100107836
弁理士　西　和哉
(74)代理人　100108453
弁理士　村山　靖彦

最終頁に続く

(54)【発明の名称】プラントにおけるセキュリティ脅威レポートを作成する方法及びシステム

(57)【特許請求の範囲】
【請求項１】
プラントデータネットワークに接続される複数のヒューマンインターフェースステーションにおけるセキュリティ脅威レポートを作成する方法であって、
a)比較分析レポートツールのスケジューラが、前記ヒューマンインターフェースステーションからセキュリティ脅威データを収集するスケジュールを設定するステップと、
b)比較分析レポートツールが、前記スケジューラによって割り当てられた所定のスケジュールに基づき、前記ヒューマンインターフェースステーション(複数可)からセキュリティ脅威データを収集するステップと、
c)前記比較分析レポートツールが、収集された前記セキュリティ脅威データを記憶装置に格納するステップと、
d)前記比較分析レポートツールが、重要業績評価指標(KPI)を取得するために格納された前記セキュリティ脅威データに対して指標計算を実行するステップと、
e)前記比較分析レポートツールが、前記KPIに基づきセキュリティ脅威レポートを作成するステップと
を具備し、
前記スケジュールを設定するステップは、
前記比較分析レポートツールのスケジューラが、前記セキュリティ脅威データを収集すべき前記ヒューマンインターフェースステーションを選択し、この選択したヒューマンインターフェースステーションに応じて収集すべき所定の種類のセキュリティ脅威データを

設定することを備え、
前記指標計算を実行するステップは、
前記比較分析レポートツールが、所定期間に収集された前記セキュリティ脅威データの検出件数の総和を前記所定期間を表す最小単位の総和で除算して前記KPIを計算することを特徴とする方法。
【請求項２】
前記セキュリティ脅威レポートは比較可能なスケールでKPIを示すことを特徴とする請求項１に記載の方法。
【請求項３】
前記セキュリティ脅威データは、権限のないユーザのログオン試み、USB挿入又は取り外し、及び、前記プラントデータネットワークへの未知の接続、又は、これらの組み合わせを包含するグループから選択されることを特徴とする請求項１に記載の方法。
【請求項４】
前記所定のスケジュールは、セキュリティ脅威データを収集する時間、セキュリティ脅威データを収集するヒューマンインターフェースステーションのロケーション、又は、これらの組み合わせを包含するグループから選択されることを特徴とする請求項１に記載の方法。
【請求項５】
プラントデータネットワークに接続される複数のヒューマンインターフェースステーションにおけるセキュリティ脅威レポートを作成するシステムであって、
a)スケジュールに従って前記ヒューマンインターフェースステーションからセキュリティ脅威データを収集するプロセスを開始するためのスケジューラと、
b)収集された前記セキュリティ脅威データの重要業績評価指標(KPI)を計算するように構成された演算装置と、
c)収集された前記セキュリティ脅威データ及び前記KPIを格納するための記憶装置と、
d)前記KPIに基づき前記セキュリティ脅威レポートを作成するための手段と
を備え、
前記スケジューラは、
前記セキュリティ脅威データを収集すべき前記ヒューマンインターフェースステーションを選択し、この選択したヒューマンインターフェースステーションに応じて収集すべき所定の種類のセキュリティ脅威データを設定するように構成され、
前記演算装置は、
所定期間に収集された前記セキュリティ脅威データの検出件数の総和を前記所定期間を表す最小単位の総和で除算して前記KPIを計算するように構成されることを特徴とするシステム。
【請求項６】
前記スケジューラは、要求されたスケジュールに従ってプログラム可能であることを特徴とする請求項５に記載のシステム。
【請求項７】
前記セキュリティ脅威レポートは、好ましくは、スプレッドシートを使用して作成されることを特徴とする請求項５に記載のシステム。
【請求項８】
前記セキュリティ脅威レポートは、グラフ表示を包含することを特徴とする請求項５に記載のシステム。
【請求項９】
プラントデータネットワークに接続される複数のヒューマンインターフェースステーションにおけるセキュリティ脅威レポートを作成させるためのコンピュータプログラムであって、
前記ヒューマンインターフェースステーションからセキュリティ脅威データを収集するスケジュールを設定するステップと、

設定された前記スケジュールに基づき、前記ヒューマンインターフェースステーション(複数可)からセキュリティ脅威データを収集するステップと、
収集された前記セキュリティ脅威データを記憶装置に格納するステップと、
重要業績評価指標(KPI)を取得するために格納された前記セキュリティ脅威データに対して指標計算を実行するステップと、
前記KPIに基づきセキュリティ脅威レポートを作成するステップと
を実行させ、
前記スケジュールを設定するステップは、
前記セキュリティ脅威データを収集すべき前記ヒューマンインターフェースステーションを選択し、この選択したヒューマンインターフェースステーションに応じて収集すべき所定の種類のセキュリティ脅威データを設定することを備え、
前記指標計算を実行するステップは、
所定期間に収集された前記セキュリティ脅威データの検出件数の総和を前記所定期間を表す最小単位の総和で除算して前記KPIを計算することを特徴とすることが可能なコンピュータプログラム。
【請求項１０】
プラントデータネットワークに接続される複数のヒューマンインターフェースステーションにおけるセキュリティ脅威レポートを作成させるための命令を記録したコンピュータ読み取り可能な記録媒体であって、
前記ヒューマンインターフェースステーションからセキュリティ脅威データを収集するスケジュールを設定するステップと、
設定された前記スケジュールに基づき、前記ヒューマンインターフェースステーション(複数可)からセキュリティ脅威データを収集するステップと、
収集された前記セキュリティ脅威データを記憶装置に格納するステップと、
重要業績評価指標(KPI)を取得するために格納された前記セキュリティ脅威データに対して指標計算を実行するステップと、
前記KPIに基づきセキュリティ脅威レポートを作成するステップと
を実行させ、
前記スケジュールを設定するステップは、
前記セキュリティ脅威データを収集すべき前記ヒューマンインターフェースステーションを選択し、この選択したヒューマンインターフェースステーションに応じて収集すべき所定の種類のセキュリティ脅威データを設定することを備え、
前記指標計算を実行するステップは、
所定期間に収集された前記セキュリティ脅威データの検出件数の総和を前記所定期間を表す最小単位の総和で除算して前記KPIを計算することを特徴とすることが可能なコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、工業オートメーションプラントにおけるセキュリティ関連情報の比較分析サービスに関する。セキュリティ脅威レポートを作成するためにプラントのデータネットワークを使用する。
【背景技術】
【０００２】
セキュリティ関連情報は工業オートメーションプロセスにとり非常に重要である。相当の注意がセキュリティ関連情報に払われない場合、プラントの生産性は重大に影響を受け得る。したがって、セキュリティ関連情報は工業プラントの進歩にとり非常に重要である。現在の実務では、プラントの機能の生産性を低下させることでシステムを害する可能性がある。また、プラントのパフォーマンス及びタイムリーな製品配送に影響を与える脆弱なアクティビティのため、リソースが適切に利用されない可能性がある。

【０００３】
現在、プラントのセキュリティを評価し、かつ、向上させるために使用することができる重要業績評価指標(Key performance Index: KPI)を作成し、かつ、計算するために、工業オートメーション領域でセキュリティ関連データを収集するための当該技術分野における方法は存在しない。
【発明の概要】
【課題を解決するための手段】
【０００４】
本発明は、プラントデータネットワークにおけるセキュリティ脅威レポートを作成するための方法を提供する。これは、ネットワークにおける選択された又はすべてのヒューマンインターフェースステーション(Human Interface Station)についてスケジューラを設定するステップと、前記スケジューラによって割り当てられた所定の制約に基づき、前記ネットワークの前記ヒューマンインターフェースステーション(複数可)からセキュリティ脅威データを収集するステップと、収集された前記データを記憶装置に格納するステップと、KPIを取得するために格納された前記データに対して指標計算を実行するステップと、前記重要業績評価指標に基づきセキュリティ脅威レポートを作成するステップとを含んでいるが、これに限定されない。
【０００５】
したがって、１態様は、プラントデータネットワークにおけるセキュリティ脅威レポートを作成するためのシステムを提供する。これは、スケジュールに従ってセキュリティ脅威データを収集するプロセスを開始するためのスケジューラを含んでいるが、これに限定されない。また、それは、収集された前記データのKPIを計算するように構成された演算装置を備えている。さらに、それは、収集された前記データ及び前記重要業績評価指標を格納するための記憶装置と、前記指標に基づき前記セキュリティ脅威レポートを作成する手段とを備えている。
【０００６】
当業者には他の多数の態様が明らかであり、本発明の態様は、以降に、以下の説明及び添付の特許請求の範囲から明白になる。
【図面の簡単な説明】
【０００７】
【図１】本明細書に説明された方法が適用されるシステムを図示している。
【図２】セキュリティ脅威レポートを作成するためのシステムの代表的な実施例を示している。
【図３】スケジューラにおけるスケジュールの例を示している。
【図４】所定の期間における権限のないユーザのログオン試みの数に関するセキュリティ脅威レポートの例を示している。
【図５】プラントにおけるセキュリティ脅威レポートを作成する1実施例のフローチャートを示している。
【発明を実施するための形態】
【０００８】
以下の詳細な説明では、その一部を構成する添付図面が参照される。図面では、コンテキストが別の方法を指示しない限り、類似記号は同様のコンポーネントを通常特定する。詳細な説明で説明された代表的な実施例、図面、および特許請求の範囲は限定することを意図するものではない。本明細書に提示された本発明の真の趣旨又は範囲を逸脱することなく、他の実施例を利用してもよく、かつ、他の変更がなされてもよい。
【０００９】
プラントデータネットワークにおけるセキュリティ脅威レポートを作成する方法のために提供された本発明は、
a)前記ネットワークにおける選択された又はすべてのヒューマンインターフェースステーション102についてスケジューラ107を設定するステップと、

b)前記スケジューラ107によって割り当てられた所定の制約に基づき、前記ネットワークの前記ヒューマンインターフェースステーション(複数可)からセキュリティ脅威データを収集するステップと、
c)収集された前記データを記憶装置106に格納するステップと、
d)重要業績評価指標(KPI)を取得するために格納された前記データに対して指標計算を実行するステップと、
e)前記KPIに基づきセキュリティ脅威レポートを作成するステップと
を具備している。

【００１０】
１実施例では、前記レポートは比較可能なスケールでKPIを示す。

【００１１】
１実施例では、前記セキュリティ脅威データは、権限のないユーザのログオン試み、USB挿入又は取り外し、及び、前記ネットワークへの未知の接続、又は、これらの組み合わせを包含するグループから選択される。

【００１２】
１実施例では、前記所定の制約は、時間、データ、及び、セキュリティ脅威、又は、これらの組み合わせを包含するグループから選択される。

【００１３】
１実施例では、本発明は、
a)スケジュールに従ってセキュリティ脅威データを収集するプロセスを開始するためのスケジューラ107と、
b)収集された前記データの重要業績評価指標(KPI)を計算するように構成された演算装置と、
c)収集された前記データ及び前記KPIを格納するための記憶装置106と、
d)前記指標に基づき前記セキュリティ脅威レポートを作成するための手段と
を備えたプラントデータネットワークにおけるセキュリティ脅威レポートを作成するシステムを提供する。

【００１４】
１実施例では、前記スケジューラ107は、要求されたスケジュールに従ってプログラム可能である。

【００１５】
好ましくは、１実施例では、前記レポートはスプレッドシートを使用して作成される。

【００１６】
１実施例では、前記レポートはグラフ表示を包含する。

【００１７】
１実施例では、本発明は、前記ネットワークにおける選択された又はすべてのヒューマンインターフェースステーション102についてスケジューラ107を設定するステップと、前記スケジューラ107によって割り当てられた所定の制約に基づき、前記ネットワークの前記ヒューマンインターフェースステーション(複数可)102からセキュリティ脅威データを収集するステップと、収集された前記データを記憶装置106に格納するステップと、重要業績評価指標(KPI)を取得するために格納された前記データに対して指標計算を実行するステップと、前記KPIに基づきセキュリティ脅威レポートを作成するステップとを実行させることが可能なプラントデータネットワークにおけるセキュリティ脅威レポートを作成させるためのコンピュータプログラムを提供する。

【００１８】
１実施例では、本発明は、前記ネットワークにおける選択された又はすべてのヒューマンインターフェースステーション102についてスケジューラ107を設定するステップと、前記スケジューラ107によって割り当てられた所定の制約に基づき、前記ネットワークのヒューマンインターフェースステーション(複数可)102からセキュリティ脅威データを収集するステップと、収集された前記データを記憶装置106に格納するステップと、重要業績

評価指標(KPI)を取得するために格納された前記データに対して指標計算を実行するステップと、前記KPIに基づきセキュリティ脅威レポートを作成するステップとを実行可能なプラントデータネットワークにおけるセキュリティ脅威レポートを作成させるための命令を記録したコンピュータ読み取り可能な記録媒体を提供する。

【００１９】

本発明は、プラント運転及び生産性を向上させるための解決法を提供する。それは、プラント運転における危険なアクティビティを特定し、かつ、それを是正するために相当の対策を実施するのに役立つ。図1は、HIS01、HIS02、HIS03等からHISnまでのHISを包含するヒューマンインターフェースステーション(HIS)グループ102を示している。これらのHISは、プラント運転を伴う人間のアクティビティの相互作用ポイントである。一例として、これらは、パーソナルコンピュータ(PC)又は制御装置又は入力可能な組み込み機器を備えた機械である。比較分析レポートツール(Comparative Analysis Report Tool: CART)PC101は、プラントデータネットワークに接続されて、HIS102を監視する。CART PC101は、プラントネットワークにおける、それぞれのHISの危険なアクティビティを特定する。この場合、プラントネットワークは、私設ネットワーク(例えば、ローカルエリアネットワーク(LAN)など)、又は、公衆ネットワーク(例えば、インターネット、ワールドワイドウェブなど)、又は、それらの組み合わせ(例えば、仮想私設ネットワーク、インターネットに接続されたLANなど)を包含する。その上、ネットワークは、有線ネットワークだけである必要はなく、かつ、当技術分野で既知のようにワイヤレスネットワーク要素を包含してもよい。

【００２０】

図2を参照すれば、CART PC101は、セキュリティ脅威データ(権限のないログオンユーザの詳細、未知の接続、すべてのヒューマンインターフェースステーション102からのUSBデバイスの挿入及び取り外しを含んでいるが、これに限定されない)を収集する。アクティビティを実行するためのスケジュールはスケジューラ107によって定義される。収集されたセキュリティデータは記憶装置106に格納される。指標計算機能103は、記憶装置106からの収集されたセキュリティデータに基づき指標を作成する。比較及びレポート機能104は、プラントパフォーマンスの比較レポートの図表を作成する。このレポートは、どんな脅威でもプラント脆弱性を特定するのに役立つ。さらに、スケジューラ107、記憶装置106、指標計算機能103、比較及びレポート機能104が単一のPCに存在する必要はない。

【００２１】

図2は、CARTを備えたシステムの１実施例のより詳細な図を示している。この実施例では、システムは、PCにロードされたCARTアプリケーションを有する。HISグループ102は、CARTアプリケーションと相互作用するHIS01から始まりHISnまでのHISを有する。スケジューラ107は、スケジュールに従ってITセキュリティ機能105を起動するために使用されるサービスである。ITセキュリティ機能105は、スケジューラ設定に基づき、権限のないユーザのアクセス、未知の接続の詳細、及び、USBの挿入/取り外しのようなセキュリティ脅威データを収集する。スケジューラ107は、スケジューラ107サービスによって、いつITセキュリティ機能を起動するかを記述するのに使用されるスケジュールで設定される。スケジュールは、データを収集しなければならない日付、時間、期間、脅威データを収集しなければならないHISロケーション/アドレス/ID、及び、ITセキュリティ機能105を起動するためにスケジューラ107によって要求される他の情報を含んでいるが、これに限定されない。また、スケジュールは、特定の危険なアクティビティデータ(即ち、セキュリティ脅威データ)を収集しなければならない定期的な間隔を記述する。これは、スケジューラ107のスケジュールによって記述されるように、ITセキュリティ機能105を起動することを結果として生じさせる。

【００２２】

これから図3を参照すれば、それはスケジューラ107を設定する例を示している。図はすべてのHISに適用可能なスケジュールを図示している。設定に従って、スケジューラ107は、毎日22:30にすべてのヒューマンインターフェースステーションからセキュリティ脅威

データを収集するためのITセキュリティ機能105を起動し始める。この例は、1回で、すべてのセキュリティ脅威データ機能を起動する場合を説明する。また、スケジュールに示されたように所定のセキュリティ脅威データを収集するそれらのITセキュリティ機能だけを起動させるように、スケジューラ107をプログラムすることも可能である。１実施例では、スケジューラ107は、選択されたセキュリティ脅威データが選択されたHIS又はHISのグループについて収集されるように構成することができる。異なったHISのグループが異なったセキュリティ脅威データを収集させるようにプログラムすることができる。例えば、セキュリティ脅威データがHIS101及びHIS102から毎日午前10時30分に収集され、かつ、HIS103、HIS104から毎週日曜日の午後10時に収集されるように、設定を行うことができる。さらに、どんなHISからのUSBの挿入/取り外しも24時間体制で監視しなければならないことが要求される場合がある。したがって、スケジューラ107は、USBの挿入/取り外しに関する情報が、それが発生する限り、収集されるように設定することができる。

【００２３】

ITセキュリティ機能105によって収集されたすべてのデータが、記憶装置106に格納される。記憶装置106は、特定の形式でデータを格納可能なデータベースである。例えば、データベースは、Oracle(登録商標)又はSQL又は読み出し可能な形式でデータを格納可能な他の代替手段である。

【００２４】

指標計算機能ブロック103は、記憶装置106から格納されたデータを収集する。それは、ITセキュリティ機能105によって各HISから収集されたデータに基づきKPIを計算するために使用される指標計算式を有する。

【００２５】

１実施例では、権限のないユーザのログオン試みに使用される計算式は以下の通りである。

$$KPI=\Sigma(At_1+At_2+At_3+\cdots+At_n)/n \qquad (1)$$

ここで、

Atiは、1日あたりの権限のないユーザのログオン試みの数であり(ここで、i=1...n)、

ｎは、分析期間の日数である。

【００２６】

別の実施例では、未知の接続に使用される計算式は以下の通りである。

$$KPI=\Sigma(At_1+At_2+At_3+\cdots+At_n)/n \qquad (2)$$

ここで、

Atiは、1日あたりのヒューマンインターフェースステーションにおける未知の接続の数であり(ここで、i=1...n)、

ｎは、分析期間の日数である。

【００２７】

さらに別の実施例では、USBデバイスの挿入/取り外しに使用される計算式は以下の通りである。

$$KPI=\Sigma(At_1+At_2+At_3+\cdots+At_n)/n \qquad (3)$$

ここで、

Atiは、1日あたりのヒューマンインターフェースステーションにおけるUSB接続のカウントであり(ここで、i=1...n)、

ｎは、分析期間の日数である。

【００２８】

権限のないユーザのログオン試みに関する詳細は、HISのユーザグループの一員でなく、かつ、それにログオンしようとするそれらのユーザから収集される。また、HISの認定ユーザがログオンするために誤ってユーザ名/パスワードを入力した場合、そのような試みに関する詳細も収集される。例えば、表1は、2008年の間に起こった権限のないユーザのログオン試みの数をリスト化している。このデータを収集するために採用される方法のうちの1つは、HISからのWindows（登録商標）イベントビューア(Windows Event viewer)

ーセキュリティ監査セクション(Security Audit section)からのそれを収集する方法によって実施することができる。しかしながら、容易に他の様々な既知の方法を代用することができることがよく理解される。

【００２９】

【表１】

表 1

ヒューマンインターフェーススステーション(HIS)	収集日	権限のないユーザのログオン試みのカウント
HIS 101	2008 年 5 月 1 日	3
HIS 102	2008 年 6 月 15 日	2
HIS 103	2008 年 9 月 12 日	8
HIS 104	2008 年 12 月 25 日	4

【００３０】

権限のないユーザのログオン試みに対するKPIを計算するために、上記した式(1)と、表１からの値とを使用することによって、KPI値は以下の通り計算される。

KPI= (3+2+8+4)/4

KPI=4.25

2008年のKPI値は「4.25」である。

【００３１】

同様に、未知の接続情報を収集することは、CARTアプリケーションの一部として扱われないHISで行われた新しいネットワーク接続に基づいている。例えば、表2は2008年の間に起こった未知の接続をリスト化している。このデータを収集するために採用される方法のうちの1つは、Netstatアプリケーションを実行する方法によって実施することができる。しかしながら、容易に他の様々な既知の方法を代用することができることがよく理解される。

【００３２】

【表２】

表 2

ヒューマンインターフェーススステーション	アクセス時間	ポート	ローカルアドレス	フォーリンアドレス	関係した実行可能
HIS 101	5/5/2008 10:15:00	630	192.169.191.10	192.169.16.10	Abc.exe
HIS 102	5/6/2008 10:15:00	550	192.169.191.11	192.169.16.10	Xyz.exe

【００３３】

未知の接続に対するKPIを計算するために、上記した式(2)と、表2からの値とを使用することによって、KPI値は以下の通り計算される。

KPI= (1+1)/2

KPI=1
2008年のKPI値は「1」である。
【００３４】
同様に、CARTは、連続的にそれを観察することによって、それぞれのヒューマンインターフェースステーションへのUSBデバイス挿入/取り外しの数を収集する。連続的な監視のため、スケジュールは必要ではないか、又は、スケジューラ107はHISを連続的に観察するのに役立つ方法でプログラムされる。スケジューラは、HISを特定の期間及び時間にわたって監視しなければならない場合に設定することができる。ユーザがUSBデバイス(例えば、フラッシュメモリデバイス、キーボード、マウスなど)を挿入する/取り外すと、USB挿入/取り外しイベントがトリガされる。このトリガデータは取得され、かつ、記憶装置106に格納される。表3は2008年の間に起こったUSB挿入/取り外し情報の例のリストを示している。
【００３５】
【表３】

表 3

ヒューマンインターフェースステーション(HIS)	アクセス時間	挿入/取り外し
HIS 101	5/5/2008 10:15:00	1 –USB デバイス挿入
HIS 101	5/5/2008 10:20:00	0 –USB デバイス取り外し
HIS 103	5/6/2008 11:30:00	1 – USB デバイス挿入
HIS 103	5/6/2008 1:30:00	0 – USB デバイス取り外し
HIS 103	5/6/2008 22:00:00	1 – USB デバイス挿入
HIS 103	5/6/2008 23:30:00	0 – USB デバイス取り外し

【００３６】
USBに対するKPIを計算するために、上記した式(3)と、表3からの値とを使用することによって、KPI値は以下の通り計算される。
HIS101へのUSBデバイスの挿入/取り外しの数は１であり、
HIS103へのUSBデバイスの挿入/取り外しの数は2である場合、
KPI= (1+2)/2
KPI=1.5
2008年のKPI値は「1.5」である。
【００３７】
１実施例では、比較及びレポート機能ブロック104が、数年の間でKPIデータを比較し、かつ、好ましくは、スプレッドシート形式でレポートを作成するために使用される。スプレッドシート(１又は複数のチャート、表、グラフ、行列、テキスト、及び、他の組合せとして表されたKPIデータを含む)の形でレポートを作成することができる。レポートは、テキストだけであるか、又は、グラフ表示又はその組み合わせを具備してもよい。レポート作成は、要求に従ってどんな形式であってもよく、かつ、スプレッドシートのみに限定はされない。
【００３８】
例えば、表4は、異なった数年間の権限のないユーザのログオン試みの数に対するKPIデータを示している。
【００３９】

【表４】

表 4

年	KPI データ
2006	10
2007	20
2008	3

【００４０】

上記したKPIデータを比較し、かつ、セキュリティ脅威レポートのExcel(登録商標)チャートを作成する比較及びレポート機能ブロック104の例が図4に示されている。それは、2007年に、権限のないユーザによって行われた試みの数に顕著な上昇があることを示している。これは、プラントの生産性及び製品のタイムリーな配送を妨げるHISにおける一部の脆弱なアクティビティを見つけ出すのに役立つ。また、それは、状況を容易に理解するのに役立ち、かつ、プラントでのプロセスを改良するのに役立つプラントパフォーマンスの比較レポートの図表を提供する。

【００４１】

図5は、プラントデータネットワークにおけるセキュリティ脅威レポートを作成するための方法の１実施例を要約するフローチャートを示している。ステップ501は、スケジューラ107が設定されるかをチェックする。スケジュールが利用可能でない場合、次いで、スケジューラ107が設定されるまで待機する。ステップ502では、スケジューラ107は要求に従ってスケジュールを用いて設定される。スケジュールは、ネットワークにおける選択されたHIS、又は、すべてのHISを目的とすることができる。いったんスケジューラ107が設定されると、ステップ503では、セキュリティ脅威データが、スケジュールで定義されたように、ネットワークのヒューマンインターフェースステーション(複数可)102から収集される。しかしながら、要求がセキュリティ脅威データを24時間収集することである場合、スケジューラ107はプログラムされる必要はない。例えば、HISからUSB挿入/取り外しデータを収集する場合である。ステップ503では、収集されたデータは記憶装置106に格納される。この格納されたデータは、ステップ504で、KPIを計算するのに役立つ。ステップ505で、KPIに基づくセキュリティ脅威レポートが作成される。

【００４２】

システムは、すべてのヒューマンインターフェースステーションにおいて別々のCARTクライアントアプリケーション(HISのセキュリティ関連情報をCARTアプリケーションに提供する)を開発及び展開するためにさらに強化してもよい。本発明でKPI計算に使用された計算式は、可能性のある実施例のうちの1つである。格納された値を処理するために、これらの計算式を変更するか、又は、取り替えることができることが容易に理解される。計算式へのそのような変更が当業者にとって本発明の範囲の中にまだ含まれることがよく理解される。

【００４３】

本発明は、この出願で説明された特定の実施例(種々の態様の例証であると意図される)で制限してはならない。当業者に明らかであるように、多くの変形例及び変更例はその真の趣旨及び範囲から逸脱することなく実施することができる。本明細書に列挙されたものに加えて、機能上、本発明の範囲と同等な方法及びシステムが以上の説明から当業者に明らかである。そのような変形例及び変更例は、添付された特許請求の範囲に含まれることが意図されている。本発明は、そのような特許請求の範囲が与える均等物のすべての範囲と共に、添付された特許請求の範囲によってのみ制限しなければならない。

【００４４】

実質的に、複数及び/又は単数の用語の本明細書における使用について、当業者は、コンテキスト及び/又はアプリケーションに応じて適切に、複数から単数へ、及び/又は、単数から複数へ翻訳することができる。様々な単数/複数の置換えは明瞭性のために本明細書において明示的に説明される。

【００４５】

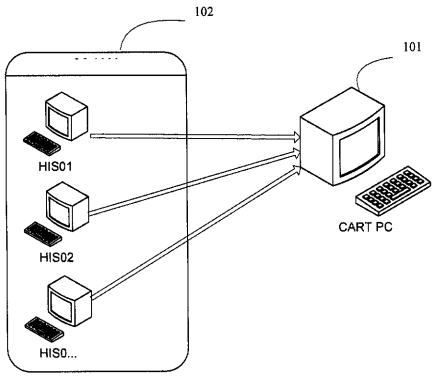
さらに、本発明の特徴又は態様がマーカッシュ(Markush)群で説明され、当業者は、また、本発明が、個別の要素又はマーカッシュ群の要素サブグループで、それによって説明されることを理解する。

【符号の説明】

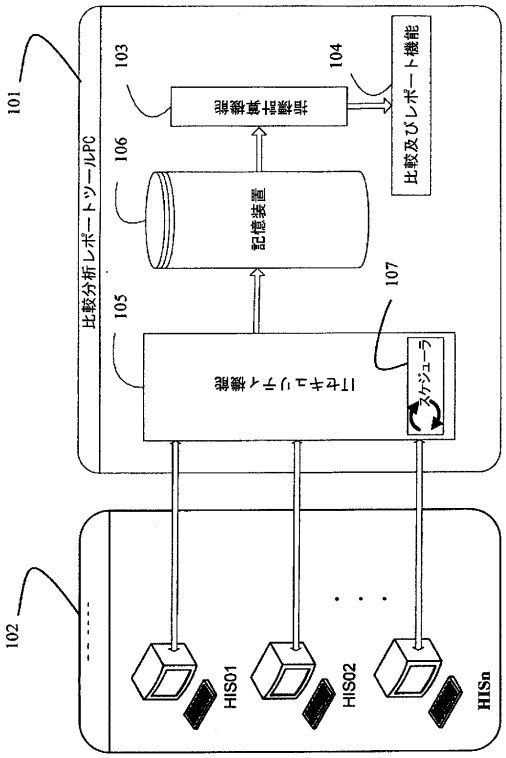
【００４６】

101　比較分析レポートツールPC
102　HIS
103　指標計算機能
104　比較及びレポート機能
105　ITセキュリティ機能
106　記憶装置
107　スケジューラ

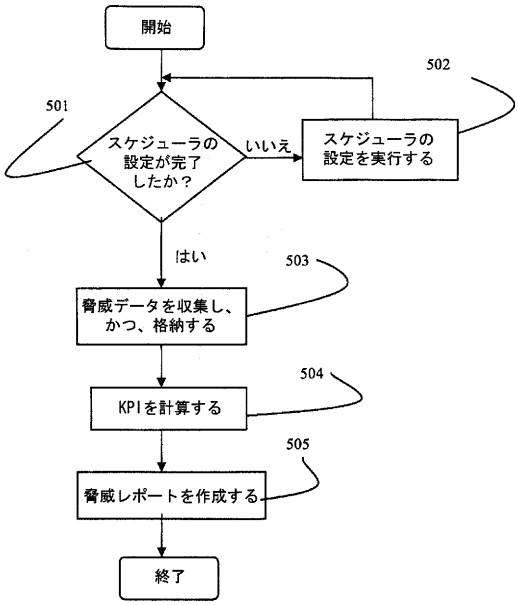
【図１】



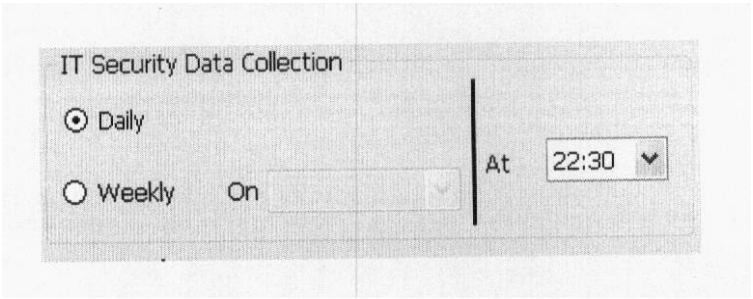
【図２】



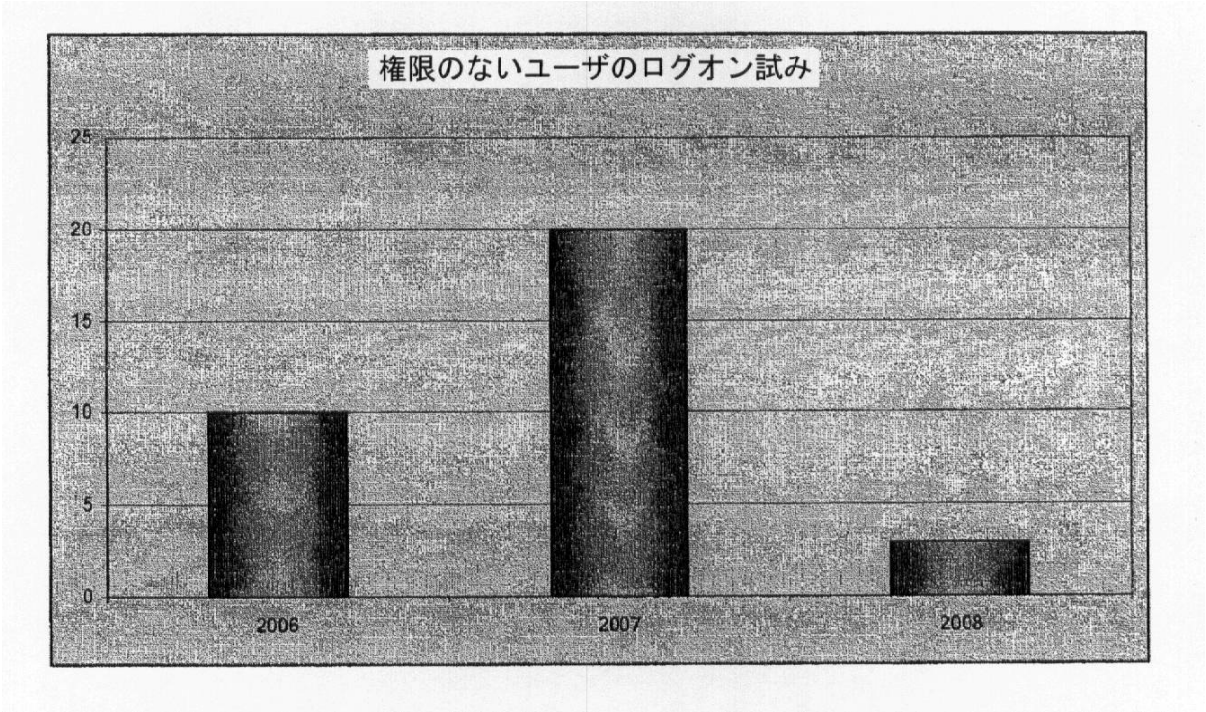
【図５】


開始
502
501
スケジューラの設定が完了したか？
いいえ
スケジューラの設定を実行する
はい
503
脅威データを収集し、かつ、格納する
504
KPIを計算する
505
脅威レポートを作成する
終了

【図３】


IT Security Data Collection
Daily
Weekly
On
At
22:30

【図４】



フロントページの続き

(72)発明者　ジョティ・バスカラン・カリアムージー
インド・カルナタカ・５６００６６・バンガロー・ホワイトフィールド・ロード・（番地なし）・インターナショナル・テック・パーク・ナヴィゲーター・ビルディング・フォース・フロアー・ユニット・４・ヨコガワ・アイエー・テクノロジーズ・インディア・プライヴェート・リミテッド内

審査官　松野　広一

(56)参考文献　特開２００９－００９５３８（ＪＰ，Ａ）
特開２００７－２４１５１３（ＪＰ，Ａ）
特開２００７－０６５７７３（ＪＰ，Ａ）
特表２００５－５１５５４１（ＪＰ，Ａ）
特開２００６－２７９３３８（ＪＰ，Ａ）
鈴木 秀一　外１名，ソリューション提案　コンプライアンス対応ログ管理の決定版　ＳＩＭツール，ネットワーク　マガジン，日本，株式会社アスキー，２００６年１２月　１日，第１１巻　第１２号，ｐｐ．１３０－１３３
古川 泰弘　外１名，ペネトレーションテスト入門，日本，ソフトバンククリエイティブ株式会社　新田　光敏，２００６年１２月３１日，第1版，ｐｐ．１９８－２０２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　　１０／００－５０／３４