(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7538136号
(P7538136)

(45)発行日　令和6年8月21日(2024.8.21)

(24)登録日　令和6年8月13日(2024.8.13)

(51)国際特許分類
Ｇ０６Ｆ　21/55　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/55　３４０

請求項の数　20　（全24頁）

(21)出願番号　特願2021-552559(P2021-552559)
(86)(22)出願日　令和2年3月10日(2020.3.10)
(65)公表番号　特表2022-523965(P2022-523965A)
(43)公表日　令和4年4月27日(2022.4.27)
(86)国際出願番号　PCT/US2020/021901
(87)国際公開番号　WO2020/185785
(87)国際公開日　令和2年9月17日(2020.9.17)
審査請求日　令和5年2月21日(2023.2.21)
(31)優先権主張番号　62/817,304
(32)優先日　平成31年3月12日(2019.3.12)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/439,421
(32)優先日　令和1年6月12日(2019.6.12)
最終頁に続く

(73)特許権者　511077292
ユニバーサル シティ スタジオズ リミテッド ライアビリティ カンパニー
アメリカ合衆国 カリフォルニア州 ９１６０８ ユニバーサル シティ ユニバーサル シティ プラザ １００
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100086771
最終頁に続く

(54)【発明の名称】　セキュリティ機器拡張

(57)【特許請求の範囲】
【請求項１】
電子装置であって、
１又は２以上のプロセッサを含む組み込み型コンピュータを備え、前記１又は２以上のプロセッサは、
セキュリティ機器から、保護コンポーネントに関連するセキュリティイベントをそれぞれが示す１又は２以上のセキュリティイベントメッセージを受け取り、
前記１又は２以上のセキュリティイベントメッセージにおける第１のコードから、前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの指示を識別し、前記第１のコードは複数のコードの予め決められたリストのうちの１つであり、前記複数のコードの各々は前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムのそれぞれのタイプを指定するために使用され、
前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの前記識別に少なくとも部分的に基づいて前記１又は２以上のセキュリティイベントメッセージの第１の独自の深刻度特性評価を識別し、前記第１の独自の深刻度特性評価は、前記複数のコードの前記予め決められたリストの第２のコードによって指定される前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第２のタイプの指示に少なくとも部分的に基づいて識別される第２の独自の深刻度特性評価とは異なり、
前記第１の独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御

動作を決定し、
　前記１又は２以上の提示又は制御動作を実行する、
ように構成される、
ことを特徴とする電子装置。
【請求項２】
前記第１の独自の深刻度特性評価は、前記セキュリティ機器によって受け取られた前記１又は２以上のセキュリティイベントメッセージの１又は２以上の特性を前記組み込み型コンピュータによって予想される特定の独自の深刻度特性評価にマッピングするマッピングスクリプトを実行することによって決定される、
請求項１に記載の電子装置。
【請求項３】
前記セキュリティ機器によって受け取られた前記１又は２以上のセキュリティイベントメッセージの前記１又は２以上の特性は第１の深刻度レベルを含み、前記組み込み型コンピュータによって予想される前記特定の独自の深刻度特性は第２の深刻度レベルである、
請求項２に記載の電子装置。
【請求項４】
前記組み込み型コンピュータの前記１又は２以上のプロセッサは、前記マッピングスクリプトを実行するように構成される、
請求項２に記載の電子装置。
【請求項５】
前記第１の独自の深刻度特性評価は、前記セキュリティ機器から受け取られる、
請求項２に記載の電子装置。
【請求項６】
ディスプレイを備え、前記１又は２以上の提示又は制御動作は、
前記ディスプレイ上のグラフィカルユーザインターフェイス（ＧＵＩ）を介して、前記第１の独自の深刻度特性評価に基づいて、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上のアラームバナーを提示すること、又は、
スタックライトを介して、前記第１の独自の深刻度特性評価に基づいて、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上の視覚的アラーム指示を提示すること、又は、
これらの両方、
を含む、請求項１に記載の電子装置。
【請求項７】
前記１又は２以上の提示又は制御動作は、前記保護コンポーネントの動作状態を修正することを含む、
請求項１に記載の電子装置。
【請求項８】
前記保護コンポーネントは、娯楽アトラクションを含む、
請求項７に記載の電子装置。
【請求項９】
前記１又は２以上のセキュリティイベントメッセージは、メッセージロギングのためのＳｙｓｌｏｇ標準に従って生成されたメッセージを含む、
請求項１に記載の電子装置。
【請求項１０】
前記電子装置のオペレータから１又は２以上の入力／出力（Ｉ／Ｏ）コマンドを受け取り、又は前記オペレータに１又は２以上の出力指示を提供し、又はこれらの両方を行うように構成された１又は２以上のＩ／Ｏ装置と、
　前記１又は２以上のＩ／Ｏコマンドを示すＩ／Ｏデータを受け取って前記１又は２以上のＩ／Ｏコマンドを実行し、又は、
　前記１又は２以上の出力指示を受け取り、前記１又は２以上のＩ／Ｏ装置を介して前

記１又は２以上の出力指示を提示し、又は、
　これらの両方を行う、
ように構成されたプログラマブルロジックコントローラ（ＰＬＣ）と、
を備える、請求項１に記載の電子装置。
【請求項１１】
前記１又は２以上のＩ／Ｏ装置は、前記第１の独自の深刻度特性評価の指示を提供する１又は２以上のライトの組を含み、
前記１又は２以上のライトの組は、第１の状態の時に危機的深刻度セキュリティイベントを、第２の状態の時に中深刻度セキュリティイベントを選択的に示す障害発光ダイオード（ＬＥＤ）を含み、
前記１又は２以上のライトの組は、全ての予想されるインターフェイスが前記電子装置に通信可能に結合されているかどうかを示す正常発光ダイオード（ＬＥＤ）を含む、
請求項１０に記載の電子装置。
【請求項１２】
前記組み込み型コンピュータは、
前記ＰＬＣの変数の継続的に変化する状態が前記組み込み型コンピュータにおいて閾値時間内に検出されない時を判定し、
前記継続的に変化する変数の状態を前記閾値時間内に検出しなかったことに応答して、前記組み込み型コンピュータの機能不全を示す障害を提供する、
ように構成される、請求項１０に記載の電子装置。
【請求項１３】
前記１又は２以上のＩ／Ｏ装置は、実行／迂回スイッチを含み、該実行／迂回スイッチは、
実行モードの場合、前記１又は２以上のセキュリティイベントメッセージが受け取られた時に、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上のアラームバナーをログ記録させて提示させ、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上のアラームを提示させ、
迂回モードの場合、前記１又は２以上のセキュリティイベントメッセージが受け取られた時に、前記１又は２以上のセキュリティイベントメッセージに関連する前記１又は２以上のアラームバナーをログ記録させて提示させ、前記１又は２以上のセキュリティイベントメッセージに関連する前記１又は２以上のアラームの提示を控えさせる、
請求項１０に記載の電子装置。
【請求項１４】
前記１又は２以上のＩ／Ｏ装置は、リセットモードに設定された時に前記組み込み型コンピュータの電源を落とし、又は再起動させ、又はこれらの両方を行わせるリセットスイッチを含む、
請求項１０に記載の電子装置。
【請求項１５】
有形の非一時的コンピュータ可読媒体であって、コンピュータシステムの１又は２以上のプロセッサによって実行された時に、
セキュリティ機器から、保護コンポーネントに関連するセキュリティイベントをそれぞれが示す１又は２以上のセキュリティイベントメッセージを受け取ることと、
前記１又は２以上のセキュリティイベントメッセージにおける第１のコードから、前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの指示を識別することであって、前記第１のコードは複数のコードの予め決められたリストのうちの１つであり、前記複数のコードの各々は前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムのそれぞれのタイプを指定するために使用される、ことと、
前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの前記識別に少なくとも部分的に基づいて前記１又は２以上のセキュリティイベン

トメッセージの第１の独自の深刻度特性評価を識別することと、
前記第１の独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御動作を決定することであって、前記第１の独自の深刻度特性評価は、前記複数のコードの前記予め決められたリストの第２のコードによって指定される前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第２のタイプの指示に少なくとも部分的に基づいて識別される第２の独自の深刻度特性評価とは異なる、ことと、
前記１又は２以上の提示又は制御動作を実行することと、
を前記コンピュータシステムに行わせるコンピュータ可読命令を含む、ことを特徴とするコンピュータ可読媒体。
【請求項１６】
前記１又は２以上のプロセッサによって実行された時に、前記セキュリティ機器によって受け取られた前記１又は２以上のセキュリティイベントメッセージの１又は２以上の特性を前記コンピュータシステムによって予想される特定の独自の深刻度特性評価にマッピングするマッピングスクリプトを実行することによって前記第１の独自の深刻度特性評価を識別することを前記コンピュータシステムに行わせるコンピュータ可読命令を含む、
請求項１５に記載のコンピュータ可読媒体。
【請求項１７】
前記１又は２以上のプロセッサによって実行された時に、前記１又は２以上のセキュリティイベントメッセージに対応する１又は２以上のアラームバナーと、前記１又は２以上のセキュリティイベントメッセージの前記第１の独自の深刻度特性評価の指示とを前記コンピュータシステムのグラフィカルユーザインターフェイス（ＧＵＩ）内に提示することを前記コンピュータシステムに行わせるコンピュータ可読命令を含む、
請求項１５に記載のコンピュータ可読媒体。
【請求項１８】
前記１又は２以上のプロセッサによって実行された時に、
プログラマブルロジックコントローラ（ＰＬＣ）の変数の継続的に変化する状態が前記コンピュータシステムにおいて閾値時間内に検出されない時を判定することと、
前記継続的に変化する変数の状態を前記閾値時間内に検出しなかったことに応答して、前記コンピュータシステムの機能不全を示す障害を提供することと、
を前記コンピュータシステムに行わせるコンピュータ可読命令を含む、請求項１５に記載のコンピュータ可読媒体。
【請求項１９】
保護コンポーネントに関連するセキュリティイベントをそれぞれが示す１又は２以上のセキュリティイベントメッセージを、セキュリティ機器からコンピュータシステムを介して受け取ることと、
前記１又は２以上のセキュリティイベントメッセージにおける第１のコードから、前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの指示を識別することであって、前記第１のコードは複数のコードの予め決められたリストのうちの１つであり、前記複数のコードの各々は前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムのそれぞれのタイプを指定するために使用される、ことと、
前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第１のタイプの前記識別に少なくとも部分的に基づいて前記１又は２以上のセキュリティイベントメッセージの第１の独自の深刻度特性評価を、前記コンピュータシステムを介して識別することであって、前記第１の独自の深刻度特性評価は、前記複数のコードの前記予め決められたリストの第２のコードによって指定される前記１又は２以上のセキュリティイベントメッセージをログ記録するプログラムの第２のタイプの指示に少なくとも部分的に基づいて識別される第２の独自の深刻度特性評価とは異なる、ことと、
前記第１の独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御動作を決定することと、

前記１又は２以上の提示又は制御動作を実行することと、
を含むことを特徴とするコンピュータに実装された方法。
【請求項２０】
グラフィカルユーザインターフェイス（ＧＵＩ）を介して、前記第１の独自の深刻度特性評価に基づいて、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上のアラームバナーを提示すること、又は、
スタックライトを介して、前記第１の独自の深刻度特性評価に基づいて、前記１又は２以上のセキュリティイベントメッセージに関連する１又は２以上の視覚的アラーム指示を提示すること、又は、
これらの両方、
を含む、請求項１９に記載のコンピュータに実装された方法。
【発明の詳細な説明】
【技術分野】
【０００１】
〔関連出願との相互参照〕
本出願は、２０１９年３月１２日に出願された「セキュリティ機器拡張（ＳＥＣＵＲＩＴＹ　ＡＰＰＬＩＡＮＣＥ　ＥＸＴＥＮＳＩＯＮ）」という名称の米国仮特許出願第６２／８１７，３０４号の利益を主張するものであり、この文献の開示は全ての目的で引用により本明細書に組み入れられる。
【０００２】
本開示は、一般にセキュリティ機器に関する。具体的には、本開示のいくつかの実施形態は、セキュリティログ内に生成されたイベントの特性評価に基づいて特定の動作を実行するユーザインターフェイスに関する。
【背景技術】
【０００３】
デジタル時代には、デジタルデータの蔓延によって、これらのデジタルデータを保護する任務を負うサイバーセキュリティの必要性が増してきている。通常、セキュリティオペレーションセンター（ＳＯＣ）又はネットワークオペレーションセンター（ＮＯＣ）にはサイバーセキュリティ脅威がもたらされ、ここではサイバーセキュリティチームがこれらのサイバーセキュリティ脅威をモニタし、優先順位付けして是正する任務を負う。しかしながら、残念なことに、サイバーセキュリティ脅威の数が増加の一途をたどるにつれ、人間の主観に依拠してこれらの脅威の優先順位付け及び是正を行うことは次第に非効率的になっている。従って、人間の主観という非効率性を抱えない改善されたサイバーセキュリティイベントの優先順位付け、提示及び是正措置を提供することが必要とされている。
【０００４】
本節は、以下で説明及び／又は特許請求する本技術の様々な態様に関連し得る技術の様々な態様を読者に紹介するためのものである。本考察は、読者に背景事情を示して本開示の様々な態様のより良い理解を促す上で役立つと考えられる。従って、これらの記載は、先行技術を認めるものとしてではなく、上記の観点から読むべきものであると理解されたい。
【発明の概要】
【課題を解決するための手段】
【０００５】
以下、当初の特許請求の範囲の主題と同一範囲のいくつかの実施形態を要約する。これらの実施形態は、本開示の範囲を限定するものではなく、むしろいくつかの開示する実施形態の概要を示すものにすぎない。実際には、本開示は、以下に示す実施形態と類似し得る又は異なり得る様々な形態を含むことができる。
【０００６】
本明細書で説明する実施形態は、セキュリティイベントを効率的に受け取って優先順位付けし、これらのセキュリティイベントに基づいてセキュリティイベント動作を実行する

セキュリティ機器拡張に関する。具体的には、独自の深刻度特性評価マッピング（ｃｕｓｔｏｍｉｚｅｄ ｓｅｖｅｒｉｔｙ ｃｈａｒａｃｔｅｒｉｚａｔｉｏｎ ｍａｐｐｉｎｇ）に基づいてセキュリティイベントを特性評価する。イベントの独自の深刻度特性評価を使用して、動作のために実行すべき特定の動作セットを決定する。

【０００７】

一例として、ある実施形態では、電子装置が、１又は２以上のプロセッサを有する組み込み型コンピュータを含む。プロセッサは、セキュリティ機器から、保護コンポーネントに関連するセキュリティイベントをそれぞれが示す１又は２以上のセキュリティイベントメッセージを受け取る。プロセッサは、１又は２以上のセキュリティイベントメッセージの独自の深刻度特性評価を識別し、独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御動作を決定する。その後、プロセッサによって１又は２以上の提示又は制御動作が実行される。

【０００８】

ある実施形態では、有形の非一時的コンピュータ可読媒体がコンピュータ可読命令を含む。コンピュータの１又は２以上のプロセッサによって命令が実行されると、コンピュータは、セキュリティ機器から１又は２以上のセキュリティイベントメッセージを受け取る。１又は２以上のセキュリティイベントメッセージの各々は、保護コンポーネントに関連するセキュリティイベントを示す。さらに、コンピュータの１又は２以上のプロセッサによって命令が実行されると、コンピュータは、１又は２以上のセキュリティイベントメッセージの独自の深刻度特性評価を識別し、独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御動作を決定し、１又は２以上の提示又は制御動作を実行する。

【０００９】

ある実施形態では、コンピュータに実装された方法が、セキュリティ機器からコンピュータを介して１又は２以上のセキュリティイベントメッセージを受け取ることを含む。１又は２以上のセキュリティイベントメッセージの各々は、保護コンポーネントに関連するセキュリティイベントを示す。方法は、コンピュータを介して、１又は２以上のセキュリティイベントメッセージの独自の深刻度特性評価を識別することも含む。独自の深刻度特性評価は、少なくとも１又は２以上のセキュリティイベントメッセージに示される深刻度へのマッピングに基づいて識別される、コンピュータによって予想される深刻度を含む。方法は、識別された独自の深刻度特性評価に基づいて実行すべき１又は２以上の提示又は制御動作を決定することと、１又は２以上の提示又は制御動作を実行することと、をさらに含む。

【００１０】

全体を通じて同じ部分を同じ符号によって示す添付図面を参照しながら以下の詳細な説明を読めば、本開示のこれらの及びその他の特徴、態様及び利点がより良く理解されるであろう。

【図面の簡単な説明】

【００１１】

【図１】本開示の実施形態による検出及び対応セキュリティシステム（ＤＲＳＳ）を示す概略図である。

【図２】本開示の実施形態による、セキュリティイベントを特性評価するプロセスを示すフローチャートである。

【図３】ある実施形態による、セキュリティイベント分類に基づいて提示及び制御動作を実行するプロセスを示すフローチャートである。

【図４】ある実施形態による、セキュリティ機器拡張ユーザインターフェイスの概略図である。

【図５】ある実施形態による、セキュリティ機器拡張ユーザインターフェイスの背面の概略図である。

【図６】ある実施形態による、ＤＲＳＳによるセキュリティイベントデータ収集を示すグラフィカルユーザインターフェイス（ＧＵＩ）の概略図である。

【図７】ある実施形態による、セキュリティイベントを提示するＤＲＳＳのＧＵＩの概略図である。
【図８】ある実施形態による、特殊機能にログインするためのＤＲＳＳのＧＵＩの概略図である。
【図９】ある実施形態による、ログイン後に特殊機能を提示するＤＲＳＳのＧＵＩの概略図である。
【図１０】ある実施形態による、エラーを提示するＤＲＳＳのＧＵＩの概略図である。
【発明を実施するための形態】
【００１２】
以下、本開示の１又は２以上の具体的な実施形態について説明する。これらの説明する実施形態は、開示する技術の一例にすぎない。また、これらの実施形態を簡潔に説明するために、本明細書では実施の特徴を全て説明していない場合もある。あらゆる工学又は設計プロジェクトにおいて見られるようなあらゆるこのような実施の開発においては、実施によって異なり得るシステム関連及びビジネス関連の制約の順守などの開発者の個別の目的を達成するために、数多くの実施固有の決定を行わなければならないと理解されたい。さらに、このような開発努力は複雑で時間が掛かる場合もあるが、本開示の恩恵を受ける当業者にとっては設計、製作及び製造という日常的な取り組みであると理解されたい。
【００１３】
本開示の様々な実施形態の要素を紹介する場合、「ａ」、「ａｎ」及び「ｔｈｅ」といった冠詞は、これらの要素が１つ又は２つ以上存在することを意味するものとする。「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」及び「有する（ｈａｖｉｎｇ）」という用語は、包括的なものとして意図されており、列記する要素以外のさらなる要素が存在し得ることを意味する。また、本開示の「１つの実施形態」又は「ある実施形態」についての言及は、記載する特徴も含むさらなる実施形態の存在を排除するものとして解釈されるように意図するものではないと理解されたい。
【００１４】
本開示は、一般にサイバーセキュリティイベントの自動的な優先順位付け及び提示を行う検出及び対応セキュリティシステム（ＤＲＳＳ）に関する。ＤＲＳＳは、ユーザインターフェイスからの制御動作を容易にして、サイバーセキュリティ脅威への高速対応を可能にすることができる。このことを踏まえて、図１は、本開示の実施形態による検出及び対応セキュリティシステム（ＤＲＳＳ）１００を示す概略図である。ＤＲＳＳ１００は、保護コンポーネント１０４をモニタしているセキュリティ機器１０２によって生成されたセキュリティイベントの指示を提供する。いくつかの実施形態では、保護コンポーネント１０４を遊園地アトラクションとすることができる。セキュリティ機器１０２は、イベントのメッセージロギングによって示されることがあるサイバーセキュリティイベントについて保護コンポーネント１０４をモニタする。例えば、本明細書で使用する「Ｓｙｓｌｏｇ」は、メッセージロギングの標準を意味する。本明細書では「Ｓｙｓｌｏｇ」という用語を使用するが、本技術は数多くのメッセージロギング標準と共に機能することができ、従って「Ｓｙｓｌｏｇ」という用語の使用は、本技術をＳｙｓｌｏｇ標準に限定するように意図するものではないと理解されたい。Ｓｙｓｌｏｇメッセージロギング標準は、多くのメッセージコンポーネントを含む。例えば、Ｓｙｓｌｏｇメッセージは、メッセージをログ記録するプログラムのタイプを指定するために使用される機能コード（ｆａｃｉｌｉｔｙ　ｃｏｄｅ）を提供することができる。以下、関連するキーワード及び説明を伴う機能コードのテーブルを示す。

機能コード	キーワード	説明
０	kern	カーネルメッセージ
１	user	ユーザレベルメッセージ
２	mail	メールシステム
３	daemon	システムデーモン
４	auth	セキュリティ／認証メッセージ
５	syslog	ｓｙｓｌｏｇによって内部的に生成されたメッセージ
６	lpr	ラインプリンタサブシステム
７	news	ネットワークニュースサブシステム
８	uucp	ＵＵＣＰサブシステム
９	cron	クロックデーモン
１０	authpriv	セキュリティ／認証メッセージ

１１	ftp	ＦＴＰデーモン
１２	ntp	ＮＴＰサブシステム
１３	security	ログ監査
１４	console	ログアラート
１５	solaris-cron	スケジューリングデーモン
１６～２３	local0 - local7	ローカルに使用される機能

【００１５】
また、Ｓｙｓｌｏｇメッセージは、深刻度のリストを含むことができる。以下、Ｓｙｓｌｏｇメッセージ内に存在し得る深刻度のテーブルを示す。

値	深刻度	キーワード	非推奨キーワード	説明	状態
0	緊急	emerg	panic	システム使用不可	パニック状態
1	アラート	alert		早急に対策を取らなければならない	システムデータベース破損などの早急に是正すべき状態
2	危機的	crit		危機的状態	ハードデバイスエラー
3	エラー	err	Error	エラー状態	
4	警告	warning	warn	警告状態	
5	通知	notice		正常であるが有意な状態	エラー状態ではないが特別な扱いを必要とし得る状態
6	情報的	info		情報メッセージ	
7	デバッグ	debug		デバッグレベルメッセージ	通常はプログラムのデバッグ時にのみ役立つ情報を含むメッセージ

【００１６】
ＤＲＳＳ１００は、セキュリティ機器１０２からＳｙｓｌｏｇ出力を受け取ることができるセキュリティ機器拡張（ＳＡＥ）１０８を含むことができる。セキュリティ機器拡張１０８及び／又はセキュリティ機器１０２は、Ｓｙｓｌｏｇメッセージを翻訳することができ、従ってセキュリティ機器拡張１０８は、Ｓｙｓｌｏｇメッセージの指示の容易な解釈をもたらすグラフィカルユーザインターフェイス及び／又はスタックライト（ｓｔａｃｋ　ｌｉｇｈｔ）出力を提供することができる。Ｓｙｓｌｏｇメッセージの翻訳は、Ｓｙｓｌｏｇメッセージのコンポーネント（例えば、深刻度値及び／又は機能コード）に基づく、コンピュータに実装された独自のＳｙｓｌｏｇメッセージ深刻度特性評価を伴う。この独自の深刻度特性評価を使用して、セキュリティメッセージのネイティブな深刻度分類とは異なる深刻度特性評価を決定することができる。このことは、特定のタイプの保護コンポーネントなどに特化した独自の深刻度特性評価を構築するのに役立つことができる。例えば、遊園地アトラクションは、セキュリティイベントの深刻度特性評価がオンラインゲームサーバ環境などとは大きく異なることができる。
【００１７】
これを行うために、セキュリティ機器１０２及び／又は組み込み型コンピュータ１０６においてＳｙｓｌｏｇマッピングスクリプト１１０を実行することができる。Ｓｙｓｌｏｇマッピングスクリプト１１０は、Ｓｙｓｌｏｇメッセージの特性に従ってＳｙｓｌｏｇメッセージを特性評価する。ＳＡＥ１０８は、この特性評価に基づいてＳｙｓｌｏｇイベントのグラフィック提示を行い、及び／又はスタックライトの１又は２以上のライトを、

特定の特性評価を有するＳｙｓｌｏｇイベントを示す特定のパターンで作動させることができる。

【００１８】

ＤＲＳＳ１００は、ＳＡＥ１０８の機能を実行するために内部及び外部ソースと連動することができる。例えば、ＤＲＳＳ１００は、ＤＲＳＳ１００にＳｙｓｌｏｇメッセージを送信する外部セキュリティセンサであるセキュリティ機器１０２（例えば、Ｓｙｓｌｏｇサーバ）と連動することができる。ＤＲＳＳ１０は、着信メッセージを継続的にリスンし、メッセージの深刻度及び／又は他のメッセージ特性に従ってメッセージを処理（例えば、特性評価）することができる。

【００１９】

また、ＤＲＳＳ１００は、ドメインコントローラ１１２と連動することもできる。ドメインコントローラは、ＤＲＳＳ１００及びＳＡＥ１０８のユーザ認証を可能にすることができる。以下でさらに詳細に説明するように、ユーザ認証は、無許可のユーザが利用できないＳＡＥ１０８の機能を有効にすることができる。ドメインコントローラ１１２と連動する実施形態では、ＤＲＳＳ１００がドメインコントローラ１１２との正常な接続を継続的にチェックし、正常な接続が失われた時にアラームを発することができる。

【００２０】

さらに、ＤＲＳＳ１００は、データベース１１４にデータをログ記録することができる。例えば、データベース１１４は、Ｓｙｓｌｏｇメッセージの様々な特性評価に関連するアラーム色を構成するデータを含むテーブルを含むことができる。さらに、データベース１１４には、Ｓｙｓｌｏｇサーバから受け取られたＳｙｓｌｏｇメッセージのＳｙｓｌｏｇテーブルを、Ｓｙｓｌｏｇメッセージがいつ誰によってクリアされたかについての指示と共に維持することができる。ＤＲＳＳ１００は、データベース１１４のメンテナンスの一部として、Ｓｙｓｌｏｇテーブルをパージするクリーンアップ手順を定期的に実行することができる。

【００２１】

ＤＲＳＳ１００は、ＤＲＳＳ１００との入力／出力（ＩＯ）相互作用を取り扱うプログラマブルロジックコントローラ（ＰＬＣ）１１６を含むこともできる。ＰＬＣ１１６は、ＤＲＳＳ１００上で動作するＳＡＥ１０８アプリケーションからコマンドを受け取り、ＳＡＥ１０８のＩＯに基づいてコマンドを実行する。

【００２２】

ＤＲＳＳ１００が必ずＳｙｓｌｏｇイベント指示を提供していることを確実にするために、ＤＲＳＳ１００を継続的にモニタすることが望ましい。従って、いくつかの実施形態では、ＰＬＣ１１６の１つのタスクが、ＤＲＳＳ１００のＳＡＥ１０８アプリケーション及び／又は組み込み型コンピュータ１０６のオペレーティングシステムが機能しなくなっていないかどうかを判定するためにＤＲＳＳ１００を継続的にモニタする「ウォッチドッグ」機能を実行することである。これを行うために、ＰＬＣ１１６は、ＰＬＣ１１６内の変数の状態を継続的に変化させる。閾値期間（例えば、１０秒）内に状態変化が発生していない／ＳＡＥ１０８アプリケーションによって報告されていないことが検出されるとウォッチドッグ障害が生成され、ＤＲＳＳ１００によって対応するアラームが提示される。例えば、ウォッチドッグ障害を表す特別なスタックライト作動を提示することができる。１つの実施形態では、特別なスタックライト作動が、緑色及び青色スタックライトを消灯して黄色及び赤色スタックライトを点灯することができる。これに加えて又はこれに代えて、いくつかの実施形態では、ウォッチドッグ障害を知らせるために可聴アラームが使用される。

【００２３】

ウォッチドッグ障害をリセットするには、特別な迂回ＩＯを使用することができる。例えば、１つの実施形態では、実行／迂回キースイッチを「迂回」に切り替えてアラームを無音化することができる。「リセット」キースイッチを回転させて一定期間（例えば、少なくとも１０秒）にわたって保持すると、組み込み型コンピュータ１０６の電源を落とす

ことができる。「リセット」キーの保持を解除すると、組み込み型コンピュータ１０６が再起動する。その後に、ＤＲＳＳ１００がＳＡＥ１０８アプリケーションを再起動することができ、実行／迂回キースイッチを「実行」に切り替えて、後続のウォッチドッグ障害が迂回されないことを確実にすることができる。

【００２４】

次に、Ｓｙｓｌｏｇメッセージの特性評価について説明すると、図２は、本開示の実施形態による、セキュリティイベントを特性評価するプロセス２００を示すフローチャートである。プロセス２００は、保護コンポーネントに関連するイベント（例えば、Ｓｙｓｌｏｇメッセージ）をモニタすることによって開始する（ブロック２０２）。上述したように、Ｓｙｓｌｏｇサーバは、セキュリティイベントが発生したことを示すＳｙｓｌｏｇメッセージをＤＲＳＳ１００に提供することができる。判定ブロック２０４においてイベントが検出されない場合には、イベントが検出されるまでモニタリングが継続される。

【００２５】

イベントが検出されると、ＤＲＳＳ１００のＳｙｓｌｏｇマッピングに基づいてイベント（例えば、Ｓｙｓｌｏｇメッセージ）が特性評価される（ブロック２０６）。上述したように、この特性評価は、セキュリティ機器１０２／Ｓｙｓｌｏｇサーバ、及び／又はＤＲＳＳ１００の組み込み型コンピュータ１０６のいずれかにおいてＳｙｓｌｏｇマッピングスクリプト１１０を実行することによって行うことができる。特性評価は、Ｓｙｓｌｏｇメッセージの１又は２以上の特性を、いくつかの実施形態では深刻度４：高／危機的、深刻度３：中、及び深刻度２：低という３つの異なる深刻度レベルを含むことができるＤＲＳＳ深刻度レベルにマッピングすることができる。例えば、Ｓｙｓｌｏｇメッセージに０～２の深刻度を含むＳｙｓｌｏｇメッセージは、ＤＲＳＳ１００の目的では深刻度４の特性評価にマッピングすることができる。さらに、３～４の深刻度を含むＳｙｓｌｏｇメッセージは、ＤＲＳＳ１００の目的では深刻度３の特性評価にマッピングすることができる。５～７の深刻度を含むＳｙｓｌｏｇメッセージは、ＤＲＳＳ１００の目的では深刻度２の特性評価にマッピングすることができる。Ｓｙｓｌｏｇ深刻度を７から３深刻度の特性評価に低減することにより、優先順位付け効率の向上を認めることができる。さらに、Ｓｙｓｌｏｇマッピングスクリプト１１０は、より少ない又はより多くの深刻度レベルを提供するようにカスタマイズすることができ、Ｓｙｓｌｏｇメッセージ内で見出される数多くの項目にマッピングすることができる。例えば、ＤＲＳＳ１００では、Ｓｙｓｌｏｇ深刻度と特定の機能との組み合わせを、同じＳｙｓｌｏｇ深刻度と異なる機能コードとの組み合わせよりも高い深刻度にマッピングすることができる。

【００２６】

特性評価が決定されると、Ｓｙｓｌｏｇメッセージ（例えば、セキュリティイベント）が特性評価に関連付けられ、ＳＡＥ１０８による使用のために提供される（ブロック２０８）。この特性評価を使用して、ＳＡＥ１０８においてＳｙｓｌｏｇメッセージの提示及び／又は制御動作を実行することができる。例えば、いくつかの実施形態では、深刻度４のイベントとして特性評価されたＳｙｓｌｏｇメッセージについて、可聴アラームと共に点滅する赤色ライトを作動させることができる。さらに、ＳＡＥ１０８のグラフィカルユーザインターフェイス（ＧＵＩ）上に赤色のアラームバナーを提示することができる。また、組み込み型コンピュータ１０６によって維持される状態変数を切り替えることができる。例えば、「アラームが存在しない」ことを示す変数及び「危機的アラームが存在しない」ことを示す変数を、いずれもオフに切り替えることができる。深刻度３として特性評価されたＳｙｓｌｏｇメッセージについては、異なる動作を行うことができる。１つの実施形態では、点灯した赤色ライトが作動する。さらに、ＳＡＥ１０８のＧＵＩ上に赤色のアラームバナーを提示することができる。「アラームが存在しない」ことを示す変数をオフに切り替えることができる一方で、「危機的アラームが存在しない」ことを示す変数は、その状態を保持することができる。深刻度２として特性評価されたＳｙｓｌｏｇメッセージについては、点灯した黄色ライトを作動させることができる。ＳＡＥ１０８のＧＵＩに黄色のアラームバナーを提示することができる。「アラームが存在しない」ことを示す

変数を切り替えることができる。

【００２７】

次に、特性評価ベースの提示及び制御動作のさらに詳細な説明を行うと、図３は、ある実施形態による、セキュリティイベント分類に基づいて提示及び制御動作を実行するプロセス３００を示すフローチャートである。上述したように、セキュリティイベント（例えば、Ｓｙｓｌｏｇメッセージ）が受け取られる（ブロック３０２）。セキュリティイベントの特性評価が識別される（ブロック３０４）。例えば、プロセス２００で行われる特性評価は、データベース１１４に記憶し、セキュリティイベントの特性評価を識別するために検索することができる。

【００２８】

特性評価に基づいて、セキュリティイベントの提示及び／又は制御動作を決定することができる（ブロック３０６）。例えば、特性評価に基づいて、スタックライト／発光ダイオード（ＬＥＤ）及び／又はオーディオの作動を以下のように決定することができる。

赤色ライト－点灯	中アラーム又はウォッチドッグ障害を示す。アラームバナー上に中アラームが存在する場合にはアラームをクリアする必要がある。ＤＲＳＳ１００アプリケーションが反応しない場合にはシステムをリセットしなければならない。
赤色ライト－点滅	高／危機的アラームを示し、ＤＲＳＳ１００アプリケーション内でクリアする必要がある。
黄色ライト－点灯	低アラーム又はウォッチドッグ障害を示す。アラームバナー上に低アラームが存在する場合にはアラームをクリアする必要がある。ＤＲＳＳ１００アプリケーションが反応しない場合にはシステムをリセットしなければならない。
青色ライト－点灯	全てのインターフェイスが通信中であり、システムが「実行」モードにあることを示す。このライトが消えた場合には、実行／迂回スイッチが「迂回」に回されたか、ウォッチドッグ障害が存在する。
緑色ライト－点灯	ＰＬＣ１１６がＤＲＳＳ１００アプリケーションと通信中であり、プログラムロジックが実行中であることを示す。このライトが消えた場合には、ウォッチドッグ障害が存在し、ＤＲＳＳ１００をリセットしなければならない。
音－フラッシュ	高／危機的アラームを示し、赤色ライトと同時にフラッシュする。
音－短チャープ	新たなアラームが生成されたことを示し、オペレータの相互作用を必要とする可聴指示の役割を果たす
音－ソリッド	ウォッチドッグ障害が存在し、ＤＲＳＳ１００をリセットしなければならないことを示す。

【００２９】

以下の診断行列（ｄｉａｇｎｏｓｔｉｃ　ｍａｔｒｉｘ）には、上記のテーブルに示す作動の別の指示を示しており、今回は以下でさらに詳細に説明する実行／迂回キースイッチのＩＯキー設定も示す。また、複数の特性評価を有する複数のセキュリティイベントが同時に存在することもできる。従って、これらの多様な作動が互いに組み合わさって存在

することができる。

	A	B	C	D	E	F	G
赤色ライトー点灯				×		×	×
赤色ライトー点滅			×				
黄色ライトー点灯					×	×	×
青色ライトー点灯	×						×
緑色ライトー点灯	×	×					×
音ーフラッシュ				×	×		
音ーソリッド						×	×

Ａ：実行／迂回キースイッチが「実行モード」
Ｂ：実行／迂回キースイッチが「迂回モード」
Ｃ：高／危機的アラーム
Ｄ：中アラーム
Ｅ：低アラーム
Ｆ：ウォッチドッグ障害
Ｇ：試験灯押しボタンの押圧

上記のテーブルでは、最も左側の列にＤＲＳＳ１００のＬＥＤ及びアラーム出力の指示を示す。最上部の行には、（テーブル下方のキー項目Ａ～Ｇによって要約する）ＤＲＳＳ１００の状態の指示を示す。「×」は、ＤＲＳＳ１００のどの状態がＤＲＳＳ１００の特定のＬＥＤ及びアラーム出力を引き起こすかを示す。いくつかの実施形態では、このＬＥＤ及びアラーム出力のテーブル及びその対応するＤＲＳＳ１００状態が、回路内に実装されるロジック及び／又はＤＲＳＳ１００によって実装される機械可読命令の表現である。

【００３０】

正しい提示及び／又は制御動作を決定すると、これらの提示及び／又は制御動作がＤＲＳＳ１００によって実行される（ブロック３０８）。例えば、以下でさらに詳細に説明するように、スタックライトは、ユニットの背面の端子ブロックを介してＤＲＳＳに配線することができる。ＬＥＤは、共通指示を表示するようにまとめてスタックライトに配線することができる。

【００３１】

図４は、ある実施形態による、スタックライト４０２を含むセキュリティ機器拡張（ＳＡＥ）パネル４００の概略図である。ＳＡＥパネル４００は、外部ソース（例えば、Ｓｙｓｌｏｇサーバ）から受け取られたシステムアラームをオペレータに通知し、任意に外部システムと連動して保護コンポーネント１０４を外部制御することができる。実行すべきアラーム動作が識別されると、ＤＲＳＳ１００は、必要なＬＥＤ４０４及びスタックライト４０２モジュールを作動させる。さらに、ＳＡＥ１０８／ＤＲＳＳ１００アプリケーションを表示して、セキュリティイベント及びその関連する特性評価を示すアラームバナーを含むグラフィカルユーザインターフェイス（ＧＵＩ）を提供するディスプレイ４０６上に、アラーム指示を提示することができる。ディスプレイ４０６は、オペレータがセキュリティイベントをクリアし、以下でさらに詳細に説明するような他の制御動作を実行することを可能にするタッチ画面とすることができる。

【００３２】

ＳＡＥパネル４００は、キースイッチ４０３を含むことができる。迂回キースイッチ４０３Ａは、スイッチが２つの位置のどちらに対応しているかに応じてＳＡＥ１０８を実行モード又は迂回モードのいずれかの状態に入れる２位置キースイッチである実行／迂回キースイッチである。迂回モードでは、制御インターフェイス出力が現在のアラームを無視してＯＮに維持される。ＤＲＳＳ１００アプリケーションは、アラームを表示してログ記録し続ける。実行モードでは、本明細書で説明したような受け取られたセキュリティイベ

ントに基づいて制御インターフェイス出力が作動する。
【００３３】
さらに、リセットスイッチ４０３Ｂを設けることもできる。上述したように、リセットスイッチ４０３Ｂは、回転させて一定期間（例えば、少なくとも１０秒）保持することによって組み込み型コンピュータ１０６の電源を落とすことができるキースイッチとすることができる。「リセット」キーの保持を解放すると、組み込み型コンピュータ１０６が再起動する。
【００３４】
ＬＥＤ４０４についてさらに詳細に説明すると、ＬＥＤ４０４Ａは、第１の状態（例えば、点滅）の時には危機的セキュリティイベント特性評価を示し、第２の状態（例えば、点灯）の時には中セキュリティイベント特性評価を示す障害ＬＥＤである。ＬＥＤ４０４Ｂは、低アラーム特性評価を示す警告ＬＥＤである。ＬＥＤ４０４Ｃは、全てのインターフェイスが接続されており、実行／迂回キーが「迂回位置」ではなく「実行」位置にあることを示す正常ＬＥＤである。ＬＥＤ４０４Ｄは、ＰＬＣ１１６が接続されてＩＯロジックを実行していることを示すＩＯ接続ＬＥＤである。
【００３５】
次に、ＳＡＥ１０８の外部インターフェイスを参照すると、図５は、ある実施形態によるＳＡＥパネル４００の背面の概略図である。図示のように、ＳＡＥパネル４００は、ＳＡＥパネル４００に空気流を提供する冷却ファン５０２を含む。
【００３６】
ＳＡＥパネル４００は、組み込み型コンピュータ１０６をＳｙｓｌｏｇサーバ（例えば、図１のセキュリティ機器１０２）に通信可能に結合するために使用される、ここではＲＪ４５イーサネットポートである第１の通信ポート５０４を含む。上述したように、Ｓｙｓｌｏｇサーバは、最終的には本明細書で説明したような提示及び／又は制御動作をトリガする特性評価されたセキュリティイベントになるＳｙｓｌｏｇメッセージを提供する。
【００３７】
ＳＡＥパネル４００は、組み込み型コンピュータ１０６を図１のドメインコントローラ１１２に通信可能に結合するために使用される、ここではＲＪ４５イーサネットポートである第２の通信ポート５０６も含む。上述したように、ドメインコントローラ１１２は、ユーザ認証を容易にして、以下でさらに詳細に説明するような保護制御機能を可能にすることができる。
【００３８】
ＳＡＥパネル４００は、スタックライト／試験灯押しボタンインターフェイス５０８も含む。スタックライト／試験灯押しボタンインターフェイス５０８は、図４のアラームインジケータスタックライト４０２と、スタックライト４０２の診断点灯試験を実行するために押すことができる試験灯押しボタンとを接続する端子である。診断試験では、スタックライト４０２上の全てのライト及び音が瞬間的に作動する。
【００３９】
ＳＡＥパネル４００は、制御インターフェイス５１０も含む。制御インターフェイス５１０は、提示及び／又は制御動作のための可能な限りのトリガを含むようにＳＡＥパネル４００を外部インターフェイスに接続する。ＰＬＣ１１６は、制御インターフェイス５１０を介して指定出力を提供して、出力と制御インターフェイス端子ブロック上の共通端子との間の連続性を確立することができる。指定条件が満たされた場合、ＰＬＣ１１６は、出力状態を変化させて連続性を遮断する。制御インターフェイス５１０によってサポートされるリモートインターフェイス出力は、ＯＮに維持されるがいずれかのアラームが存在する場合にＯＦＦに切り替わる「アラームなし」、及びＯＮに維持されるが危機的アラームが存在する時にのみＯＦＦに切り替わる出力のペアである「危機的アラームなし」を含む。上述したように、これらの状態変化は、実行／迂回キースイッチ４０３Ａが「実行」に切り替わった時に作動する。しかしながら、実行／迂回キースイッチ４０３Ａが「迂回」に切り替わった時には、いずれかのアラームの存在にもかかわらず、アラームなし及び

危機的アラームなしの出力がＯＮに維持されるようになる。

【００４０】

いくつかの実施形態では、制御インターフェイス５１０が、保護コンポーネントの動作変化を引き起こすことができる。例えば、制御インターフェイス５１０は、娯楽アトラクションに接続し、特性評価されたセキュリティイベント／生成されたアラームに基づいて娯楽アトラクション動作を制御することができる。例えば、危機的深刻度のセキュリティイベントが提示された時には、娯楽アトラクション（例えば、乗り物）を停止させ、及び／又は他の緩和措置を取ることができる。

【００４１】

いくつかの実施形態では、ＳＡＥパネル５００が、冗長電源５１２Ａ及び５１２Ｂを含むことができる。二重電源を有することにより、電源５１２Ａ又は５１２Ｂの一方への電力が欠乏した場合でも、代替電源５１２Ａ又は５１２Ｂによって電源を維持することができる。以下でさらに詳細に説明するように、このようなイベント中には、電源５１２Ａ又は５１２Ｂのどちらが機能していないかを示すローカルアラームを提示することができる。

【００４２】

次に、ＤＲＳＳ１００／ＳＡＥ１０８アプリケーションＧＵＩについてさらに詳細に説明すると、図６は、ある実施形態による、ＤＲＳＳによって収集されたセキュリティイベントデータを示すグラフィカルユーザインターフェイス（ＧＵＩ）起動画面６００の概略図である。上述したように、ＤＲＳＳ１００アプリケーションは、着信セキュリティイベント（例えば、Ｓｙｓｌｏｇメッセージ）をリスンし、スタックライト、ＬＥＤ及びアラームバナーを介してこのようなメッセージをオペレータに通報することに関与する。このアプリケーションは、受信時間、アラームがクリアされた時間及びアラームをクリアしたユーザを含むようにアラーム履歴をログ記録することができる。上述したように、このアプリケーションは、ドメイン認証を使用してセキュリティ保護することができ、オペレーティングシステムレベルでユーザの切り替えを必要とするのではなくアプリケーションレベルで認証を行うネイティブなバリデーションＵＩを含むことができる。

【００４３】

起動画面６００に示すように、ＤＲＳＳ１００アプリケーションは、最初に起動すると、全てのシステムインターフェイスに接続する起動プロセスを実行する。インターフェイスが通信できない場合には、起動画面６００上に通信障害を示すメッセージが表示され、アプリケーションが一定期間（例えば、１０秒）後に自動的に再接続しようと試みる。初期データセット（例えば、システムインターフェイスとの通信及び／又はイベントメッセージを示すデータ）が検索されると、進捗バー６０２が、ローディングプロセスが１００％完了して起動画面６００がメイン表示画面に移行する旨を示す。ローディングプロセス中、オペレータは、ログインアフォーダンス（ｌｏｇｉｎ　ａｆｆｏｒｄａｎｃｅ）６０４を使用してログインすることができる。オペレータは、ログインすることによって、認証ユーザのみが利用できる保護動作を実行することができる。ログインプロセスについては、以下でさらに詳細に説明する。

【００４４】

図７は、ある実施形態による、ＤＲＳＳ１００アプリケーションＧＵＩのメイン表示画面７００の概略図である。メイン表示画面７００は、ＤＲＳＳ１００によって受け取られたアクティブなアラームを表示するアラームバナー７０２を提供する。アラームバナーには優先順位が付けられ、最も優先度の高いアラームが最初に提示される。さらに、バナー７０２を差別化することによってセキュリティイベントの特性評価が提供される。例えば、バナー７０２Ａは赤色バナーであり、バナー７０２Ａに関連するセキュリティアラートが深刻度３のセキュリティイベントとして特性評価されていることを示すテキスト指示を提供する。対照的に、バナー７０２Ｂ～Ｄは、それぞれ深刻度２のセキュリティイベントとして特性評価されたセキュリティイベントに関連する。

【００４５】

メイン表示画面７００上には、作動時にあらゆる現在の可聴アラームを設定可能時間（

例えば、３０秒のデフォルト時間）にわたって無音化する無音化ボタン７０４が設けられる。いくつかの実施形態では、無音化ボタン７０４がユーザ確認の作動を必要としない。しかしながら、グレーアウト表示された全クリアボタン７０６及びクリアボタン７０８によって示すように、いくつかの実施形態では、これらのオプションを（例えば、ログインボタン６０４を選択することによってログインプロセスを実行することによって）ログイン時にのみ選択することができる。

【００４６】

図８は、ある実施形態によるＧＵＩログイン画面８００の概略図である。ログイン画面８００は、オペレータによるログインクレデンシャル（例えば、ユーザＩＤ８０２及びパスワード８０４）の入力を可能にする。別の実施形態では、生体認証、物理キーなどの他のログインクレデンシャルを使用してＤＲＳＳ１００アプリケーションにログインすることができる。

【００４７】

オペレータがログインすると、全クリアボタン７０６及びクリアボタン７０８が有効になる。図９は、ある実施形態による、ログイン後に特殊機能（例えば、全クリアボタン７０６及びクリアボタン７０８）を有効にするＧＵＩメイン画面９００の概略図である。全クリアボタン７０６は、選択されると、いずれかのアラームバナー７０２の行の一切の選択にかかわらず、アラームバナー７０２によって表される全てのアラームをクリアする。クリアボタン７０８は、選択されると、選択されたアラームバナー７０２に関連するセキュリティイベントをクリアする。オペレータは、アラームバナー７０２を選択するために単純にアラームバナー７０２をタップすることができる。選択されたアラームバナー７０２は、そのアラームバナー７０２が選択されたことを示すために特性（例えば、色）を変化させる。さらに、アラームバナー７０２は、アラームバナー７０２を二度目にタップすることによって未選択にすることができる。

【００４８】

図示のように、オペレータがログインした後にはログアウトボタン９０２も提供される。ログアウトボタン９０２は、選択されるとオペレータがログアウトされる（そして、グレーアウト表示されたオプションを含むメイン画面７００が再び表示される）。

【００４９】

ＤＲＳＳ１００は、セキュリティ機器１０２から生成されたアラームを提供することに加えて、局所的イベントに基づいてアラームを生成することもできる。例えば、図１０は、ある実施形態による、エラーを提示するＤＲＳＳ１００のＧＵＩ１０００の概略図である。図示の実施形態では、ＤＲＳＳ１００によってセキュリティイベント（例えば、Ｓｙｓｌｏｇメッセージ）が受け取られていないことを示すセンサ通信障害メッセージ１００２が提示されている。ＤＲＳＳ１００アプリケーションは、セキュリティイベントが提示されない時に偽エラーが提示されないことを確実にするために、セキュリティセンサ（例えば、Ｓｙｓｌｏｇサーバ／セキュリティ機器１０２）から一定間隔でハートビートメッセージ（ｈｅａｒｔｂｅａｔ　ｍｅｓｓａｇｅｓ）を受け取ることができる。本明細書で使用するハートビートメッセージは、いつＤＲＳＳ１００によってメッセージが受け取られていないかを判定するために使用できる定期的予想メッセージである。ハートビートメッセージが検出されない場合、アプリケーションは、ハートビート障害を示すＧＵＩ１０００を提示する。ハートビートメッセージが検出されると、ＧＵＩ１０００が消えて、アプリケーションは通常動作を再開する。いくつかの実施形態では、ハートビートメッセージの間隔、及びアラーム生成前の許容可能な紛失ハートビートメッセージ数が設定可能である。

【００５０】

ＤＲＳＳ１００は、さらなるローカルアラームを含むことができる。以下は、さらなるアラーム、並びに深刻度特性評価及び説明のリストである。

アラーム名	深刻度	説明
power_supply_one	2	バックアップユニットから電源ケーブルが外れるかブレーカが作動するとこのアラームが発生する。アラームをクリアするには、電源ケーブルを差し込むかブレーカをリセットし、その後に図９のＧＵＩ９００からアラームをクリアする。
power_supply_two	2	バックアップユニットから電源ケーブルが外れるかブレーカが作動するとこのアラームが発生する。アラームをクリアするには、電源ケーブルを差し込むかブレーカをリセットし、その後に図９のＧＵＩ９００からアラームをクリアする。
circuit_breaker_tripped	2	ユニット内でブレーカが作動するとこのアラームが発生する。アラームをクリアするには、ブレーカをリセットした後に図９のＧＵＩ９００からアラームをクリアする。
domain_controller_comm	2	ドメインコントローラとの通信喪失時にこのアラームが発生する。アラームをクリアするには、ドメインコントローラとの通信を回復させた後に図９のＧＵＩ９００からアラームをクリアする。
heartbeat	2	セキュリティセンサとの通信喪失時にこのアラームが発生する。このアラームはアラームバナーとして現れるだけでなく、全画面ポップアップも表示する。アラームをクリアするには、セキュリティセンサとの通信を回復させて、ハートビートメッセージを送信中として検証する。

【００５１】

本明細書で述べたように、ＤＲＳＳ１００は、複数の用途に適した個別のアラーム提示及び制御体験をもたらす多くの方法で構成することができる。いくつかの実施形態では、ＤＲＳＳ１００アプリケーションが、アプリケーションを再インストールする必要なく構成可能パラメータをロードするＸＭＬ構成可能ファイルを含むことができる。以下は、構成パラメータ、デフォルト値及び各構成パラメータの説明のリストである。理解できるように、このリストは可能な構成パラメータの１つのリストであるが、このような構成パラメータに範囲を限定するように意図するものではない。実際には、別の実施形態におけるオプションとして、より少ない又はより多くの構成パラメータを提示することができる。

構成名	デフォルト値	説明
Title	DRSS	メイン画面上に表示されているアプリケーションのタイトルである。
DBUpdateTimeInMinutes	1	アプリケーションが標準的なアラーム色変化をチェックする時間間隔である。このパラメータを変更することは推奨されない。
HBIntervalInSeconds	5	アプリケーションが有効なハートビートをチャックすべき間隔である。セキュリティセンサ／セキュリティ機器１０２がハートビートメッセージを送信している間隔と一致すべきである。
HBAllowableMisses	4	ハートビートアラームを生成する前の最大許容可能紛失ハートビートメッセージ。
ServerIPAddress	0.0.0.0	アラームメッセージを送信しているセキュリティセンサ／セキュリティ機器１０２のＩＰアドレス。
ServerPortNumber	514	アラームメッセージ送信に利用されるポート番号。５１４はＵＤＰメッセージのための標準ポートである。
SilenceButtonInSeconds	30	無音化ボタンがクリックされた時に可聴アラームが無音化される時間。
HBEnabled	True	ハートビート機能の有効化／無効化。
DCIPAdress	0.0.0.0	ドメインコントローラのＩＰアドレス。
DCIntervalInSeconds	20	アプリケーションがドメインコントローラとの通信をチェックする間隔。

DCPingEnabled	True	ドメインコントローラ通信チェックの有効化／無効化。
AutoLogoutInSeconds	30	ユーザがアプリケーションから自動的にログアウトされる時間。
LightFlashingSpeedInMilliseconds	500	危機的アラーム時に赤色ライトが点滅する速度。
PLCIPAddress	192.168.1.121	内部ＰＬＣ１１６のＩＰアドレス。
WatchdogEnabled	True	ソフトウェアウォッチドッグロジックの有効化／無効化。
SoundChirpTimeInMilliseconds	2000	オペレータの注意を引く新たなアラームが生成された時の可聴アラームのチャープ時間。

【００５２】

本明細書に示して特許請求する技術は、本技術分野を確実に改善する、従って抽象的なもの、無形のもの又は純粋に理論的なものではない実際的性質の有形物及び具体例を参照し、これらに適用される。さらに、本明細書の最後に添付するいずれかの請求項が、「．．．［機能］を［実行］する手段」又は「．．．［機能］を［実行］するステップ」として指定されている１又は２以上の要素を含む場合、このような要素は米国特許法１１２条（ｆ）に従って解釈すべきである。一方で、他のいずれかの形で指定された要素を含むあらゆる請求項については、このような要素を米国特許法１１２条（ｆ）に従って解釈すべきではない。

【符号の説明】

【００５３】

１００　検出及び対応セキュリティシステム（ＤＲＳＳ）
１０２　セキュリティ機器
１０４　保護コンポーネント
１０６　組み込み型コンピュータ
１０８　セキュリティ機器拡張（ＳＡＥ）
１１０　Ｓｙｓｌｏｇマッピング
１１２　ドメインコントローラ
１１４　ドメインコントローラ
１１６　ＰＬＣ

【図面】

【図１】

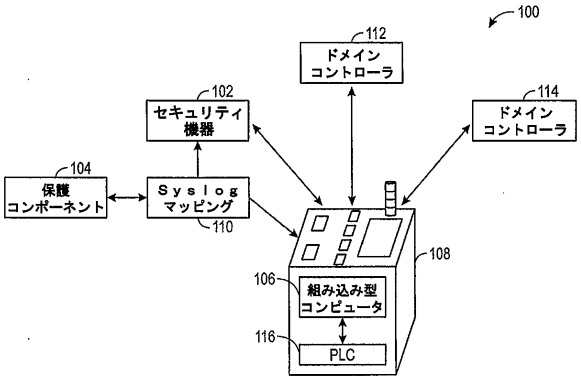

FIG. 1

【図２】

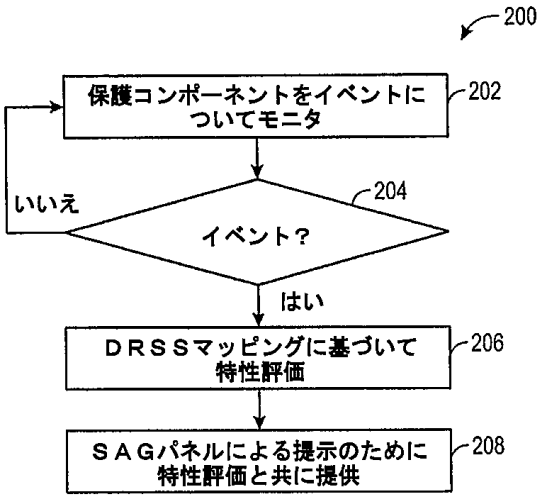

FIG. 2

【図３】

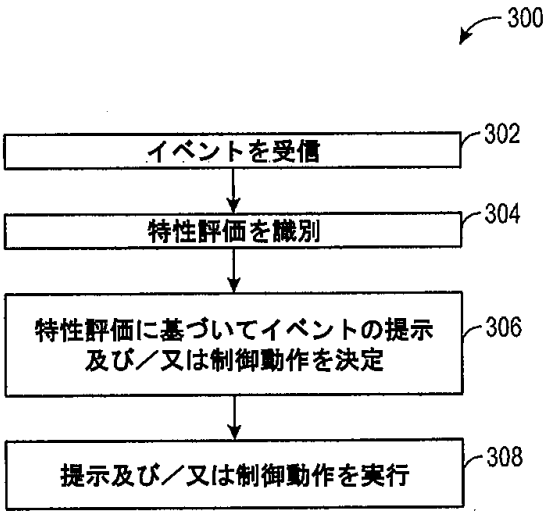

FIG. 3

【図４】

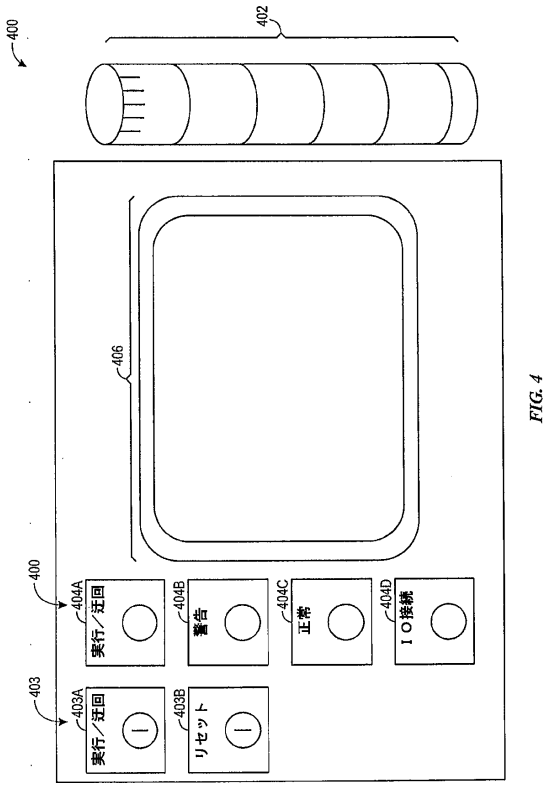

FIG. 4

【図５】

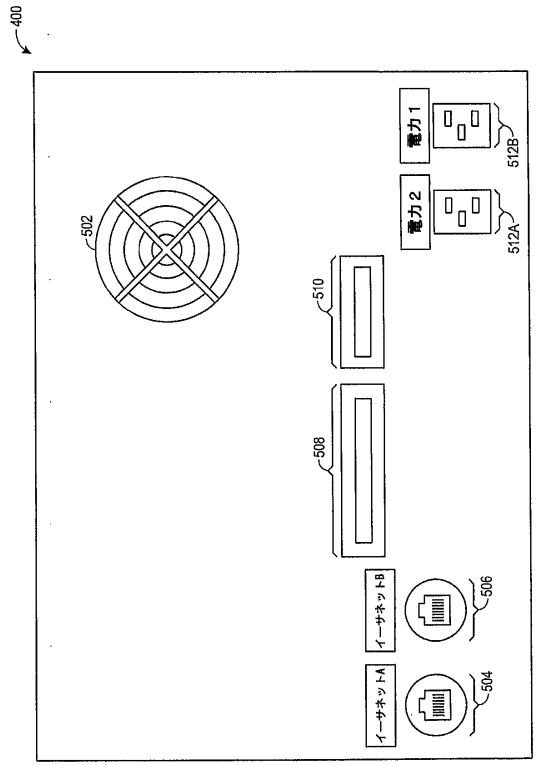

FIG. 5

【図６】

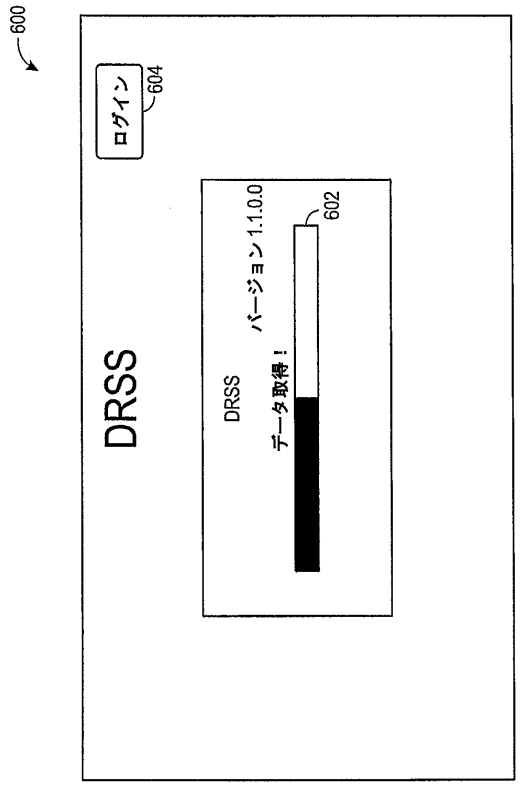

FIG. 6

【図７】

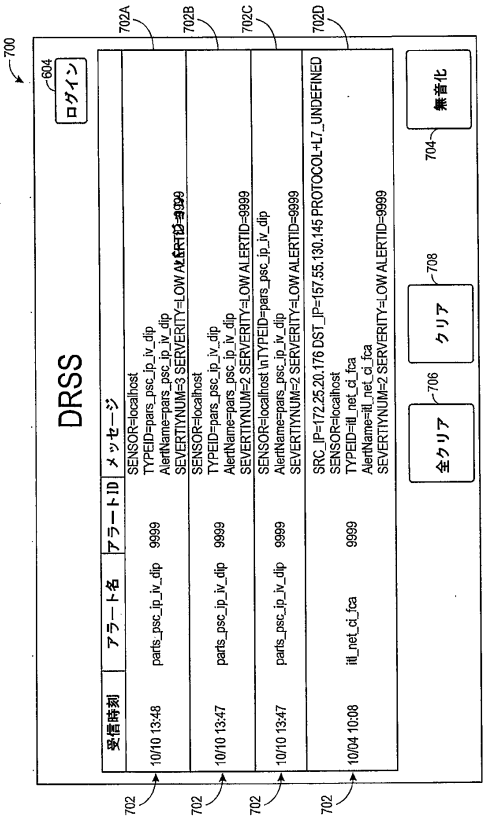

FIG. 7

【図８】

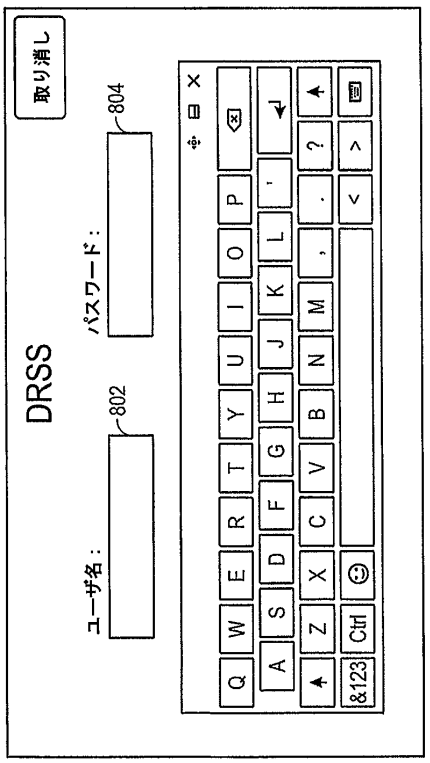

FIG. 8

【図９】

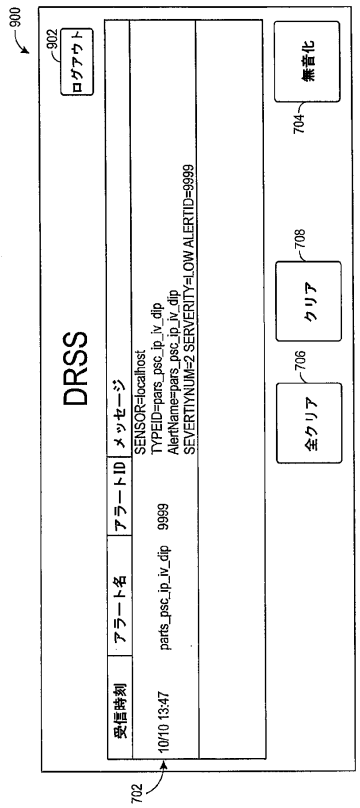

FIG. 9

【図１０】

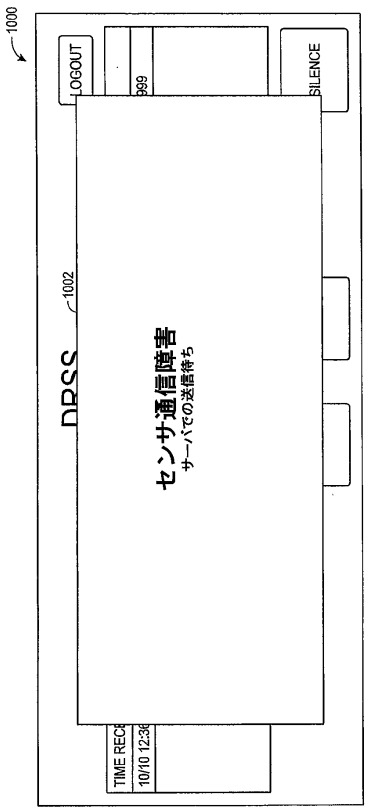

FIG. 10

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
弁理士　西島 孝喜
(74)代理人
上杉 浩
(74)代理人　100120525
弁理士　近藤 直樹
(74)代理人　100139712
弁理士　那須 威夫
(72)発明者　アウヴェス ルイス
アメリカ合衆国 フロリダ州 ３２８１９ オーランド ユニバーサル スタジオズ プラザ １０００
(72)発明者　フィッツパトリック ショーン
アメリカ合衆国 フロリダ州 ３２８１９ オーランド ユニバーサル スタジオズ プラザ １０００
(72)発明者　キング スティーヴン
アメリカ合衆国 フロリダ州 ３２８１９ オーランド ユニバーサル スタジオズ プラザ １０００
審査官　宮司 卓佳
(56)参考文献　米国特許出願公開第２００６／０１２９８７７（ＵＳ，Ａ１）
特開２０１３－１５６７８９（ＪＰ，Ａ）
特開平０８－０９５８３２（ＪＰ，Ａ）
特開２０１８－０４９６０２（ＪＰ，Ａ）
特開２０１４－２２８９３２（ＪＰ，Ａ）
特表２０１７－５３６８６１（ＪＰ，Ａ）
特開２０１１－００８４９５（ＪＰ，Ａ）
米国特許出願公開第２００７／０２３４４２６（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５