(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6923265号
(P6923265)
(45)発行日　令和3年8月18日(2021.8.18)　(24)登録日　令和3年8月2日(2021.8.2)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
H04L 12/935	(2013.01)	H04L	12/935	
G06F 21/55	(2013.01)	G06F	21/55	
G05B 23/02	(2006.01)	G05B	23/02	V

請求項の数 23　(全 33 頁)

(21)出願番号　特願2016-102096(P2016-102096)
(22)出願日　平成28年5月23日(2016.5.23)
(65)公開番号　特開2016-220213(P2016-220213A)
(43)公開日　平成28年12月22日(2016.12.22)
審査請求日　令和1年5月23日(2019.5.23)
(31)優先権主張番号　14/719946
(32)優先日　平成27年5月22日(2015.5.22)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　512132022
フィッシャー－ローズマウント　システムズ，インコーポレイテッド
アメリカ合衆国　テキサス　７８６８１－７４３０　ラウンド　ロック　ウェスト　ルイス　ヘナ　ブルバード　１１００　ビルディング　１　エマーソン　プロセス　マネージメント
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳

最終頁に続く

(54)【発明の名称】プラントセキュリティシステムにおける構成可能なロバスト性エージェント

(57)【特許請求の範囲】
【請求項１】
プロセス制御システムの通信ネットワーク内のメッセージトラフィックを安全にする方法であって、
前記通信ネットワークに接続されたデバイスで一連のメッセージを受信することと、
前記デバイスにあるプロセッサを介して、前記一連のメッセージのそれぞれを分析して、前記メッセージのそれぞれの１つ以上のメッセージ特徴を決定することと、
前記デバイスにある前記プロセッサを介して、前記デバイスで記憶されるロジックルールの組に基づいて前記メッセージのそれぞれをフィルタリングすることと、を含み、前記ロジックルールのルールは、前記デバイスへの又は前記デバイスからのメッセージトラフィックの予想される流れを反映し、前記ルールは、前記デバイスへの又は前記デバイスからのメッセージトラフィックの範囲を含むトラフィックパターンパラメータを含み、前記フィルタリングが、１つ以上の第１のメッセージ特徴の組を有するメッセージを伝達することと、１つ以上の第２のメッセージ特徴の組を有するメッセージを停止することと、前記ルールに対応する１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントすることとを含み、前記デバイスへの又は前記デバイスからのメッセージトラフィックの範囲と比較して、前記１つ以上の第３のメッセージ特徴の組と関連付けられたカウントに基づいて、前記１つ以上の第３のメッセージ特徴の組を有する前記メッセージを伝達または停止することをさらに含む、前記方法。
【請求項２】

１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントすることが、特定期間内に受信された前記第３のメッセージ特徴の組のうちの１つを有するメッセージの数をカウントすることを含む、請求項１に記載の前記方法。

【請求項３】

１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントすることが、特定期間内に受信された前記第３のメッセージ特徴の組のそれぞれの前記メッセージの数のカウントを保持することを含む、請求項１又は請求項２に記載の前記方法。

【請求項４】

前記ロジックルールを、前記デバイス内の読み出し専用メモリ、及び、読み出し／書き込みメモリの少なくとも１つに記憶することをさらに含む、請求項１～請求項３の何れか１項に記載の前記方法。

【請求項５】

前記ロジックルールの少なくとも部分を前記デバイスにあるフラッシュメモリに記憶することをさらに含む、請求項１～請求項４の何れか１項に記載の前記方法。

【請求項６】

１つ以上のログファイルを作成するために、１つ以上の停止されたメッセージに関する情報をロギングすることをさらに含む、請求項１～請求項５の何れか１項に記載の前記方法。

【請求項７】

ロギングの情報を有する前記１つ以上のログファイルを、前記通信ネットワークを介してユーザに通信することをさらに含む、請求項１～請求項６の何れか１項に記載の前記方法。

【請求項８】

前記１つ以上の第３のメッセージ特徴の組のうちの１つを有するメッセージのメッセージカウントがネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲外であるときに、アラートを生成してユーザに送信すること、及び、セキュリティ動作を起動することの少なくとも１つを行うことをさらに含む、請求項１～請求項７の何れか１項に記載の前記方法。

【請求項９】

セキュリティ動作を起動することが、前記通信ネットワーク上のデバイス内でウイルスまたは侵入検出ソフトウェアを起動すること、及び、前記通信ネットワークの通信リンクからデバイスを切断することの少なくとも１つを行うことを含む、請求項１～請求項８の何れか１項に記載の前記方法。

【請求項１０】

セキュリティ動作を起動することが、前記通信ネットワーク上の異なるデバイスを、前記通信ネットワークの通信リンクから切断することを含む、請求項１～請求項９の何れか１項に記載の前記方法。

【請求項１１】

前記１つ以上の第１のメッセージ特徴の組を有する前記メッセージを伝達すること、及び前記１つ以上の第３のメッセージ特徴の組を有する前記メッセージを伝達することが、前記デバイスで処理するために、前記メッセージを前記デバイスの通信スタックに伝達することを含む、請求項１～請求項１０の何れか１項に記載の前記方法。

【請求項１２】

前記１つ以上の第１のメッセージ特徴の組を有する前記メッセージを伝達すること、及び前記１つ以上の第３のメッセージ特徴の組を有する前記メッセージを伝達することが、前記通信ネットワーク上の別のデバイスへの伝送のために、前記メッセージを通信リンクに伝達することを含む、請求項１～請求項１１の何れか１項に記載の前記方法。

【請求項１３】

前記一連のメッセージを前記通信ネットワークに接続されたデバイスで受信することが、前記デバイス内で生成された第１の一連のメッセージを受信することと、前記通信ネッ

トワークの通信リンクから受信された第２の一連のメッセージを受信することと、を含み、前記一連のメッセージのそれぞれを分析することが、前記第１の一連のメッセージ及び前記第２の一連のメッセージのそれぞれを別個に分析することを含み、前記メッセージのそれぞれをフィルタリングすることが、前記第１の一連のメッセージ及び前記第２の一連のメッセージのそれぞれを別個にフィルタリングすることを含む、請求項１～請求項１２の何れか１項に記載の前記方法。

【請求項１４】

第１の一連のメッセージ及び第２の一連のメッセージのそれぞれを別個にフィルタリングすることが、前記第１の一連のメッセージを第１のロジックルールの組を使用してフィルタリングすることと、前記第２の一連のメッセージを第２の異なるロジックルールの組を使用してフィルタリングすることと、を含む、請求項１～請求項１３の何れか１項に記載の前記方法。

【請求項１５】

通信リンクを介して通信可能に結合されたプロセス制御システムの複数のネットワークノードを有し、前記複数のネットワークノードは、１つ以上のプロセス制御ノードを有する通信ネットワークでの使用のためのセキュリティシステムであって、

１つ以上のメッセージモジュールインターフェースであって、前記メッセージモジュールインターフェースのそれぞれが、前記ネットワークノードのうちの１つにあるプロセッサ上で実行して、前記ネットワークノードでのメッセージトラフィックを検出し、メッセージのそれぞれの１つ以上のメッセージ特徴を決定する、メッセージモジュールインターフェースと、

１つ以上のロジックルールを記憶するルールメモリであって、前記１つ以上のロジックルールは、前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの予想される流れを反映するルールを含み、前記ルールは、前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲を含むトラフィックパターンパラメータを含むことを特徴とするルールメモリと、

プロセッサ内に記憶され、かつプロセッサ上で実行され、また前記ルールメモリに結合された１つ以上のフィルタリングユニットと、を備え、前記フィルタリングユニットのそれぞれが、

構文フィルタリングモジュールと、

ボリュームフィルタリングモジュールと、

を含み、前記構文フィルタリングモジュールが、前記プロセッサ上で実行し、メッセージ特徴情報に基づいて前記ルールメモリ内に記憶された１つ以上のロジックルールを適用して、前記メッセージを伝達するか、前記メッセージを停止するか、または前記メッセージを前記ボリュームフィルタリングモジュールに伝達し、

前記ボリュームフィルタリングモジュールが、前記ルールに対応する特定のメッセージ特徴の組を有するメッセージの数をカウントして、メッセージカウントを決定し、前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲と比較して、前記メッセージカウントに基づいて前記特定のメッセージ特徴の組を有する前記メッセージを伝達するか、または前記メッセージを停止する、前記セキュリティシステム。

【請求項１６】

前記ボリュームフィルタリングモジュールに結合されているアラート生成モジュールをさらに含み、前記アラート生成モジュールが、前記プロセッサ上で実行して、前記メッセージカウントが前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲外であるときに、アラートをユーザに送信する、請求項１５に記載の前記セキュリティシステム。

【請求項１７】

前記ボリュームフィルタリングモジュールに結合されているアラート生成モジュールをさらに含み、前記アラート生成モジュールが、前記プロセッサ上で実行して、前記メッセ

ージカウントが前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲外であるときに、前記通信ネットワークからデバイスを切断する、請求項１５又は請求項１６に記載の前記セキュリティシステム。

【請求項１８】

前記１つ以上のフィルタリングユニットが、前記通信リンクから前記ネットワークノードに入ってくるメッセージを受信して分析する第１のフィルタリングユニットと、前記ネットワークノード内で生成され、前記通信リンクを介して別のネットワークノードに送信されているメッセージを受信して分析する第２のフィルタリングユニットと、を含む、請求項１５～請求項１７の何れか１項に記載の前記セキュリティシステム。

【請求項１９】

通信ネットワークであって、

通信リンクと、

プロセス制御システムの複数のネットワークノードであって、前記ネットワークノードのそれぞれが、前記通信リンクに結合されたネットワークデバイスを含み、前記複数のネットワークノードの１つ以上は、プロセス制御ノードであり、プロセッサ、及び前記プロセッサ上で実行して、前記通信リンクを行き来するメッセージを処理する通信スタックを有する、ネットワークノードと、

を備え、複数の前記ネットワークノードのそれぞれが、

１つ以上のメッセージモジュールインターフェースであって、前記メッセージモジュールインターフェースのそれぞれが、ネットワークノードにあるプロセッサ上で実行して、前記通信スタックから、または前記通信リンクから来るメッセージトラフィックを検出し、前記メッセージのそれぞれの１つ以上のメッセージ特徴を決定する、メッセージモジュールインターフェースと、

１つ以上のロジックルールを記憶する、ルールメモリであって、前記１つ以上のロジックルールは、前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの予想される流れを反映するルールを含み、前記ルールは、前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲を含むトラフィックパターンパラメータを含むことを特徴とするルールメモリと、

プロセッサ内に記憶され、かつプロセッサ上で実行され、また前記ルールメモリに結合されたフィルタリングモジュールであって、前記ルールメモリ内に記憶された前記ロジックルールの組を使用して、１つ以上の第１のメッセージ特徴の組を有するメッセージを伝達し、１つ以上の第２のメッセージ特徴の組を有するメッセージを停止し、前記ルールに対応する１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントし、また前記ネットワークデバイスへの又は前記ネットワークデバイスからのメッセージトラフィックの範囲と比較して、前記１つ以上の第３のメッセージ特徴の組と関連付けられたカウントに基づいて、前記１つ以上の第３のメッセージ特徴の組を有する前記メッセージをさらに伝達または停止する、フィルタリングモジュールと、をさらに含む、前記通信ネットワーク。

【請求項２０】

前記フィルタリングモジュールが、前記１つ以上の第３のメッセージ特徴の組を有する前記メッセージのためのメッセージカウントを、特定期間内に受信された特定のメッセージ特徴の組を有するいくつかのメッセージとして生成する、請求項１９に記載の前記通信ネットワーク。

【請求項２１】

前記複数のネットワークノードのそれぞれが、前記フィルタリングモジュールに結合されているアラート生成モジュールをさらに含み、前記アラート生成モジュールが、前記プロセッサ上で実行して、メッセージカウントのうちの１つが前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲外であるときに、アラートをユーザに送信する、請求項１９又は請求項２０に記載の前記通信ネットワーク。

【請求項２２】

前記複数のネットワークノードのそれぞれが、前記フィルタリングモジュールに結合されているアラート生成モジュールをさらに含み、前記アラート生成モジュールが、前記プロセッサ上で実行して、メッセージカウントのうちの１つが前記ネットワークノードへの又は前記ネットワークノードからのメッセージトラフィックの範囲外であるときに、通信リンクネットワークからデバイスを切断する、請求項１９～請求項２１の何れか１項に記載の前記通信ネットワーク。

【請求項２３】

前記複数のネットワークノードのそれぞれが、２つ以上のフィルタリングモジュールを含み、前記２つ以上のフィルタリングモジュールのうちの１つ目が、前記通信リンクから前記ネットワークノードにある前記ネットワークデバイスに入ってくるメッセージを受信して分析し、前記２つ以上のフィルタリングモジュールのうちの２つ目が、前記ネットワークノードにある前記ネットワークデバイス内で生成され、前記通信リンクを介して別のネットワークノードにある別のネットワークデバイスに送信されているメッセージを受信して分析する、請求項１９～請求項２２の何れか１項に記載の前記通信ネットワーク。

【発明の詳細な説明】

【技術分野】

【０００１】

本出願は、概して、プロセスまたは工業プラント通信システムに関し、より具体的に、プラント通信ネットワーク内のトラフィック検出及びフィルタリングに基づいて、制御及び保守通信ネットワーク、例えば、プロセス及び工業制御システムで使用される制御及び保守通信ネットワークへの侵入を検出することに関する。

【背景技術】

【０００２】

プロセスまたは工業制御及び保守システム、例えば、発電、化学、石油、または他の製造プロセスで使用されるプロセス制御システムのような分散または拡張可能なプロセス制御システムは、典型的に、相互に、プロセス制御ネットワークを介して少なくとも１つのホストまたはオペレータワークステーションに、及びアナログ、デジタル、または組み合わされたアナログ／デジタルバスを介して１つ以上のフィールドデバイスに通信可能に結合された１つ以上のコントローラを含む。例えば、バルブ、バルブポジショナ、スイッチ、及びトランスミッタ（例えば、温度、圧力、及び流量センサ）であり得るフィールドデバイスは、プロセスまたはプラント内で、バルブを開閉する、デバイスの電源を切り替える、及びプロセスパラメータを測定するなどの機能を実行する。コントローラは、フィールドデバイスによって行われたプロセスもしくはプラント計測及び／またはフィールドデバイスに関する他の情報を示す信号を受信し、この情報を使用して１つ以上の制御ルーチンを実装し、その後、プラントネットワークのバスまたは通信チャネル上でフィールドデバイスに送信される制御信号を生成して、プロセスまたはプラントの動作を制御する。フィールドデバイス及びコントローラからの情報は、典型的に、通信ネットワークを介して、オペレータワークステーションによって実行される１つ以上のアプリケーションに対して入手可能になり、オペレータまたは保守者が、プロセスまたはプラントに関する任意の所望の機能を実行すること、例えば、プラントの現状を見ること、プラントの動作を修正すること、デバイスを較正すること、欠陥デバイスを検出することなどを可能にする。

【０００３】

動作中、典型的にプロセスプラント環境内に位置するプロセスコントローラは、構成スキームに従い、フィールドデバイス及び／またはフィールドデバイスに関する他の情報によって行われるか、または関連付けられるプロセス計測またはプロセス変数を示す信号を定期的または規則的に受信し、この情報を使用してコントローラアプリケーションを実行するように構成される。コントローラアプリケーションは、例えば、プロセス制御決定を行い、受信された情報に基づいて制御信号を生成し、ＨＡＲＴ（登録商標）及びＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスフィールドデバイスなどのフィールドデバイス内で制御モジュールまたはブロックと連動する、異なる制御モジュールを実装する。さら

に、プロセスコントローラ内の制御モジュールは、ここでも構成スキームに従い、制御信号を通信線または他の信号パス上でフィールドデバイスに送信して、それにより、プロセスの動作を制御する。

【０００４】

フィールドデバイス及びプロセスコントローラからの情報はまた典型的に、プラント内または外部の１つ以上の他のハードウェアデバイス、例えば、オペレータワークステーション、保守ワークステーション、サーバ、パーソナルコンピュータ、携帯デバイス、データまたは事象ヒストリアン、レポートジェネレータ、集中データベースなどに対しても、１つ以上の安全なプロセス制御または保守ネットワークを介して入手可能にされる。プロセス制御または保守通信ネットワーク上で通信される情報は、オペレータまたは保守者がプロセスに関する所望の機能を実行すること、及び／またはプラントもしくはそのプラント内のデバイスの動作を見ることを可能にする。例えば、制御情報は、オペレータがプロセス制御ルーチンの設定を変更すること、プロセスコントローラまたはスマートフィールドデバイス内の制御モジュールの動作を修正すること、プロセスの現状またはプロセスプラント内の特定デバイスの状態を見ること、フィールドデバイス及びプロセスコントローラによって生成されるアラーム及び／またはアラートを見ること、人材を育成する、またはプロセス制御ソフトウェアを試験する目的でプロセスの動作をシミュレートすること、プロセスプラント内の問題またはハードウェア障害を診断することなどを許可する。

【０００５】

フィールドデバイス及びコントローラは、通常、例えば、イーサネットにより構成されたＬＡＮとして実装され得る、１つ以上の安全なプロセス制御または保守通信ネットワーク上で他のハードウェアデバイスと通信する。プロセス制御または保守通信ネットワークは、プロセスパラメータ、ネットワーク情報、及び他のプロセス制御データを、様々なネットワークデバイスを通してプロセス制御システム内の様々なエンティティに送信する。典型的なネットワークデバイスとして、ネットワークインターフェースカード、ネットワークスイッチ、ルータ、サーバ、ファイアウォール、コントローラ、オペレータワークステーション、及びデータベースが挙げられる。ネットワークデバイスは、典型的に、ルーティング、フレームレート、タイムアウト、及び他のネットワークパラメータを制御することによって、ネットワークを通るデータの流れを促進するが、プロセスデータ自体を変更しない。プロセス制御ネットワークのサイズ及び複雑性が増大するにつれて、ネットワークデバイスの数及びタイプが対応して増加する。システム及びネットワーク成長の結果として、これらの複雑なシステム内のセキュリティ及びその管理はますます困難になる。しかしながら手始めに、これらのネットワークは、一般に他の外部ネットワークから分離され、１つ以上のファイアウォールによって外的攻撃から保護される。

【０００６】

一般に、典型的な工業制御システムにおいて、ネットワークへの侵入を制限するために、プラント制御システムワークステーション／サーバは、プラントと関連付けられた様々な機能を実行する外部プラントネットワークと、制御システム内で制御及びデータ取得機能を実行する組み込み制御デバイス（例えば、コントローラ、ＰＬＣ、ＲＴＵ）との間に戦略的に配置される。制御ワークステーション／サーバの主なセキュリティ目的は、マルウェアが制御及び保守システムに侵入し、組み込みデバイスに悪影響を及ぼすのを防ぐこと、ならびにマルウェアがプラントプロセス制御データベースに記憶された構成及び履歴データを変更するのを防ぐことである。なおもさらに、これらのワークステーション／サーバは、制御システムへの不正アクセスを防いで、プラント構成の不正変更、プラントデータへの不正アクセスなどを防ぐ。ファイアウォール、「アンチウイルス」ソフトウェア、及び「ホワイトリスティング」などの多くのセキュリティ機構を使用して、これらのセキュリティ目的に対処することができるが、これらのセキュリティ機構は、典型的に十分でない。例えば、アンチウイルスソフトウェアは、「ゼロデイ」ウイルスから保護することができず、ホワイトリスティングのみが不正アプリケーションが実行するのを防ぐ。さらに、これらのセキュリティ機構は、プラントオペレータまたは予定された制御動作の活

動を妨害する可能性を有するため、これらの機構のうちのいくつかは、過度に侵入的であってプロセス制御システムでは動作上実践することができない。

【０００７】

一般的な意味において、マルウェア、例えばゼロデイ攻撃の核心部にあるマルウェアは、典型的に、プロセス制御ネットワーク内のメモリデバイス、ネットワークポート、または直接データリンクにアクセスする特権または許可を有するアプリケーションまたはサービスの動作によって、外部ネットワークへの正規の通信接続を介して安全な制御システムネットワークに導入される。代替として、マルウェアは、感染したポータブルデバイス及び／またはメディアを制御システムデバイスに接続するローカルな人員を介して安全な制御システムに導入される場合がある。その後、マルウェアは、他のデバイスに（例えば、通信を介して）伝播され得、及び／またはマルウェアに感染したアプリケーションまたはサービスのセキュリティ特権を使用して、プロセス制御ネットワーク内のデバイス内で実行され得る。さらに、このマルウェアは、それ自体がローカルに持続して、ネットワーク化されたデバイスのリブート後にそれを再度実行されるのを許可し得る。場合によって、マルウェアは、ホストの特権、例えば、感染したアプリケーションまたはサービスを、アプリケーションまたはサービスが実行されるアカウントの特権を使用して段階的に拡大し得、そうすることで、マルウェアは、より高い特権を必要とするプロセス制御デバイスまたはネットワークデバイス内でアクションまたは動作を実行可能であり得、故に、典型的に制御システム動作に対してより有害である。これらの攻撃がプラント制御システムの進行中の動作を妨害するとき、これらの攻撃は、プロセスプラント内で深刻かつ潜在的に破壊的または致命的でさえある影響を有し得る。

【０００８】

プロセスまたは工業制御及び保守ネットワークに対する攻撃を防止または制限するように動作するハードウェア及びソフトウェア構成を定義及び構築することに対して膨大な量の研究活動が行われてきた。しかしながら、堅く防御された工業制御システム（ＩＣＳ）ネットワークまたは監視制御とデータ収集（ＳＣＡＤＡ）ネットワークでさえも、依然としてセキュリティ防御の不良構成、悪意を持って行動する正当なアクセスを有するユーザ、及び外部攻撃者の代わりに行動する公的に知られていないが悪意のあるソフトウェアなどのセキュリティ脅威に曝される。さらに、一旦ネットワークが感染すると、プロセスもしくは工業制御デバイス内またはプラント通信ノード内のウイルスまたはマルウェアの存在を自動的に検出する能力が限られる。一般的に言えば、一旦プラント環境内で攻撃が成功すると、一般に、プラント通信ノードまたはデバイスが感染したことを検出するためにオペレータ、保守者などを必要とする。通信ネットワークの各ノードでバックグラウンドウイルススキャンソフトウェアを実行することが可能であるが、このソフトウェアは、大量のメモリ及び処理リソースを使い、定期的に更新される必要があり（相当のネットワーク保守リソース及び時間を要する）、依然としてゼロデイウイルスを検出することができない。

【０００９】

多くの場合、プラントデバイスまたはネットワークノードにおけるウイルスまたは不正ソフトウェアは、デバイスもしくはネットワークの性能減少を引き起こし得るか、ネットワーク内のそのノードもしくは他のノードでのエラーもしくはアラームの生成を引き起こすのに十分なほどに正常なプラント動作を中断し得るか、または他の深刻で顕著な問題を引き起こし得る。これらの場合のうちのいくつかにおいて、オペレータまたは他のプラント人員がウイルスの存在を検出することは比較的容易であり得るが、ウイルスの場所を検出することは依然として困難であり得る。さらに、多くの他の場合、ウイルスまたは攻撃は、ネットワーク動作をわずかに低下させ得る一方で、この低下またはプラント動作に対する他の影響がごくわずかになり得、そのため検出が非常に困難であり得るため、かなりの期間にわたって未検出のまま動作し得る。結果として、多くの場合、ウイルスはかなりの期間にわたって未検出になり得、その期間の間にこれらのウイルスは、プラント効率を低減するように動作し、プラントデータの窃盗を許可し、より深刻な侵入を可能にし、ネ

ットワークデバイスを深刻な攻撃または害に曝すなどし得る。

【発明の概要】

【００１０】

工業またはプロセスプラント制御または保守システムなどの制御システムは、ネットワーク上で送信された通信のロバスト分析及びフィルタリングを提供して、潜在的に感染したネットワークノードから防御する、通信ネットワーク脅威検出システムを実装する。一般的に言えば、分析システムは、ノードデバイス（例えば、コントローラ、ユーザインターフェース、スイッチなど）と、通信ネットワークとの間のインターフェースで動作する、ロバスト性エージェントを含み、ロバスト性エージェントは、ネットワークから入ってくるか、またはネットワークに向かって進むメッセージを分析及びフィルタリングして、ロバスト性エージェントを通って流れるメッセージのタイプまたはそれに関する情報を確認する。ロバスト性エージェントは、ある特定のタイプのメッセージ（例えば、ある特定の既定の特徴を有するメッセージ）がエージェントを通ってネットワークまたはデバイスに伝達されるのを許可するように構成されてよく、他の既定の特徴を有するメッセージを破棄またはフィルタリングすることによって、これらのメッセージがエージェントを通過するのを防ぐことができ、及び／または他の特徴を有するさらに他のメッセージを、ボリュームフィルターに伝達してカウントさせることができる。このボリュームフィルターは、特定のタイプの（または特定のメッセージ特徴の組を有する）メッセージの数をカウントするように動作してよく、またこれらの検出されたメッセージの数が、特定の期間にわたって特定の閾値よりも少ない場合、これらのメッセージを伝達するように動作し得るが、カウントされたメッセージの数が、特定の期間にわたって特定の閾値よりも大きい場合、これらのメッセージをフィルタリングし得る。一般的に言えば、ロバスト性エージェントは、そのフィルタリング動作が、ネットワークに対して行われた変更に基づいて経時的に変更され得、異なるタイプのネットワークまたは異なるプラント内のネットワークに対して微調整またはセットアップされ得るように構成されることができ、また一般に、ロバスト性エージェントまたは多くのロバスト性エージェントを有するセキュリティシステムが動作される任意の特定ネットワークの予想される動作に一致するように構成され得る。

【００１１】

一般的な意味で、１つ以上のそのようなロバスト性エージェントを使用するセキュリティシステムは、感染した可能性があるノードが、あるタイプであるか、または侵入と関連付けられる可能性が高い特徴を有するメッセージを伝達するのを防ぎ、感染した可能性があるノードが、侵入と関連付けられ得る相当量のメッセージをネットワーク上に送信するのを防ぐ。さらに、このシステムは、感染したノードからの攻撃下にあるノードが、侵入と関連付けられ得るか、または侵入によって引き起こされ得る、ネットワークからの相当量のメッセージを受容または受信するのを防ぐのを助ける。具体的に、セキュリティシステムのロバスト性エージェントは、（ノードからの）送信メッセージを見直して、これらのメッセージが、ネットワークの構成に基づいてネットワーク上で予想されるタイプのメッセージと対応するかどうかを決定し、例えば、アウトバウンドメッセージが、構成されたときにネットワーク通信内で予想される特徴の組を有するメッセージであるかどうかを決定する。場合によって、セキュリティシステムは、ネットワーク動作に必要であるか、または必須であると思われるタイプのメッセージを含み得る、ある特定のタイプの（またはある特定の特徴の組を有する）全てのメッセージを伝達するように構成されてよい。他の場合、セキュリティシステムは、ある特定のタイプの、またはある特定の特徴を有する全てのメッセージを拒絶またはフィルタリングするように構成されてよく、これらのメッセージは、構成されたときにネットワークの正常動作中に発生しないはずであり、したがって、システム内のマルウェアまたは感染したノードによって生成された可能性がある。第３の場合、セキュリティシステムは、ある特定のタイプの、またはある特定の特徴の組を有するメッセージを、ある特定のボリュームまたはレベルまで条件的に伝達し、その後、それらのメッセージを何らかの方法でフィルタリングするようにセットアップされ得る。この場合、この第３のタイプのある限定数のメッセージが、構成されたときにネットワ

ーク内で起こることが予想されるが、これらのメッセージは、ある特定のレベルまたはボリュームのみのこれらのメッセージが予想されることにおいて疑われることが可能である。特定期間中にある特定のレベルまたはボリュームを超えるこのタイプのメッセージの存在は、したがって、これらのメッセージがマルウェアまたはネットワークへの別のタイプの感染または侵入によって生成されることを示し得る。そのようなボリュームが検出された場合、その後、ロバスト性エージェントは、これらのメッセージの全てをフィルタリングし得るか、または限定数のこれらのメッセージを伝達し得る一方で、他をフィルタリングして、ボリュームをある特定のレベルよりも低く保持することができ、ユーザに通知することができ、侵入検出ソフトウェアを実行することができ、及び／またはメッセージを生成するデバイスをネットワークリンクから切断して、感染したデバイスがネットワークへのアクセスを有するのを防いでもよい。

【００１２】

いずれにしても、セキュリティシステムのロバスト性モジュールのそれぞれは、ボリュームフィルター内の特定の許可されるボリュームの様々なタイプのメッセージを伝達する、フィルタリングする、またはボリュームフィルターに伝達するメッセージのタイプまたは特徴を特定する構成ファイルを使用して動作するように構成されてよく、ボリューム閾値に到達するか、または超えるときなどに、ロバスト性エージェントによって措置が講じられる。この構成またはそれと関連付けられたルールは、ロバスト性エージェントまたはそのロバスト性エージェントが動作するデバイスに取り付けられた読み出し専用フラッシュメモリに記憶されてよく、これがロバスト性エージェントの動作中に構成データを変更不可能にするか、または読み出し／書き込みメモリに記憶されてよく、これがネットワークの動作中に構成を変更可能にして、したがってよりロバストにし、それにより、ネットワークに対して行われた変更に基づいて、セキュリティシステムが動作中に再構成されるのを許可する。しかしながら、後者の場合、構成ファイルは、構成ファイルを感染させるように動作することができるマルウェアの影響をより受け易いことがある。場合によって、ルールの一部がフラッシュメモリに記憶され得る一方で、ルールに使用されるいくらかのデータまたはリストは、他のタイプのメモリに構成可能な様式で記憶されてよい。

【００１３】

一般的に言えば、ロバスト性エージェントの構成は、各ロバスト性エージェントが取り付けられるネットワーク場所及びデバイスに基づいて異なってよい。さらに、任意の数のロバスト性エージェントは、ネットワークセキュリティシステムを作製するように、通信ネットワーク内に提供されてもよい。それが望ましい場合もあるが、ネットワーク内の各デバイスが必ずしもその独自のロバスト性エージェントを有する必要はない。同様に、各ロバスト性エージェントの構成は、ネットワークノードの比較的静的な構成、ならびにプラントまたはプラント制御ネットワークで使用されるプロセスまたは工業制御または保守システム構成のプライオリ性質に起因して適切に動作するようにセットアップされてよい。

【００１４】

１つ以上の実施形態では、通信リンクを介して通信的に結合された複数のネットワークノードを有する通信ネットワーク内で使用するためのセキュリティシステムは、１つ以上のメッセージモジュールインターフェースを含み、これらのメッセージモジュールインターフェースのそれぞれが、ネットワークノードのうちの１つにあるプロセッサ上で実行して、ネットワークノードでのメッセージトラフィックを検出し、メッセージのそれぞれの１つ以上のメッセージ特徴を決定する。セキュリティシステムは、１つ以上のロジックルールを記憶するルールメモリも含み、セキュリティシステムは、プロセッサに記憶され、かつプロセッサ上で実行され、またルールメモリに結合された１つ以上のフィルタリングユニットを含み、フィルタリングユニットのそれぞれが、第１のフィルタリングモジュール及び第２のフィルタリングモジュールを含む。この場合、第１のフィルタリングモジュールは、プロセッサ上で実行し、メッセージ特徴情報に基づいて、ルールメモリに記憶された１つ以上のロジックルールを適用して、メッセージを伝達するか、メッセージを停止

するか、またはメッセージを第２のフィルタリングモジュールに伝達する。さらに、第２のフィルタリングモジュールは、特定のメッセージ特徴の組を有するメッセージの数をカウントして、メッセージカウントを決定し、このメッセージカウントに基づいてメッセージを伝達するか、または特定のメッセージ特徴の組を有するメッセージを停止する。

【００１５】

所望される場合、メッセージカウントは、特定期間内に受信された特定のメッセージ特徴の組を有する特定数のメッセージを含んでよい。なおもさらに、ルールメモリは、読み出し専用メモリ、読み出し／書き込みメモリ、または読み出し専用メモリである第１の部分及び読み出し／書き込みメモリである第２の部分を含むメモリであってよい。追加として、ルールメモリは、リムーバブルフラッシュメモリなどのフラッシュメモリであってよい。

【００１６】

さらに、セキュリティシステムは、第１及び／または第２のフィルタリングモジュールに結合されたロギングモジュールを含んでよく、これがプロセッサ上で実行して、１つ以上の停止されたメッセージに関する情報を受信し、１つ以上の停止されたメッセージに関する情報をログまたはログファイルに記憶する。ロギングモジュールは、停止されたメッセージのもう１つのログをユーザに送信する通信インターフェースを含んでよく、停止されたメッセージに関するメタデータを記憶することができる。セキュリティシステムは、第２のフィルタリングモジュールに結合されているアラート生成モジュールも含み得るか、または代わりに含んでよく、アラート生成モジュールは、プロセッサ上で実行して、メッセージカウントが既定レベルに到達したときに、アラートをユーザに送信する。アラート生成モジュールは、メッセージカウントが既定レベルに到達したときに、通信ネットワークからデバイス（例えば、特定のタイプの、または特定の特徴の組を有する多数のメッセージを生成するネットワーク上の任意のデバイス）を切断するように動作してもよい。なおもさらに、１つ以上のフィルタリングユニットは、通信リンクからネットワークノードに入ってくるメッセージを受信して分析する第１のフィルタリングユニットと、ネットワークノード内で生成され、通信リンクを介して別のネットワークノードに送信されているメッセージを受信して分析する第２のフィルタリングユニットと、を含んでよい。

【００１７】

１つ以上の他の実施形態では、通信ネットワーク内のメッセージトラフィックを安全にする方法は、通信ネットワークに接続されたデバイスで一連のメッセージを受信することと、デバイスにあるプロセッサを介して、一連のメッセージのそれぞれを分析して、メッセージのそれぞれの１つ以上のメッセージ特徴を決定することとを含む。この方法は、デバイスにあるプロセッサを介して、デバイスで記憶されるロジックルールの組に基づいて、メッセージのそれぞれをフィルタリングすることをさらに含み、このフィルタリングが、１つ以上の第１のメッセージ特徴の組を有するメッセージを伝達することと、１つ以上の第２のメッセージ特徴の組を有するメッセージを停止することと、１つ以上の第３のメッセージ特徴を有するメッセージをカウントすることとを含む。さらに、この方法は、１つ以上の第３のメッセージ特徴の組と関連付けられたカウントに基づいて、１つ以上の第３のメッセージ特徴の組を有するメッセージを伝達または停止することをさらに含む。

【００１８】

さらに別の１つ以上の実施形態では、通信ネットワークは、通信リンクと、複数のネットワークノードとを含み、ネットワークノードのそれぞれが、通信リンクに結合されたネットワークデバイスを含み、プロセッサ、及びこのプロセッサ上で実行して、通信リンクを行き来するメッセージを処理する通信スタックを有する。なおもさらに、複数のネットワークノードのそれぞれは、１つ以上のメッセージモジュールインターフェースをさらに含み、メッセージモジュールインターフェースのそれぞれが、ネットワークノードにあるプロセッサ上で実行し、通信スタックから、または通信リンクから入ってくるメッセージトラフィックを検出して、メッセージのそれぞれの１つ以上のメッセージ特徴を決定する。複数のネットワークノードのそれぞれは、１つ以上のロジックルールを記憶し、プロセ

ッサに記憶され、かつプロセッサ上で実行され、またルールメモリに結合されたフィルタリングモジュールを含む、ルールメモリも含み、これがルールメモリに記憶されたロジックルールの組を使用して、１つ以上の第１のメッセージ特徴の組を有するメッセージを伝達し、１つ以上の第２のメッセージ特徴の組を有するメッセージを停止して、１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントする。フィルタリングモジュールは、１つ以上の第３のメッセージ特徴の組と関連付けられたカウントに基づいて、１つ以上の第３のメッセージ特徴の組を有するメッセージをさらに伝達または停止する。

【図面の簡単な説明】

【００１９】

【図１】プロセス制御ネットワーク内で使用され、ネットワークへの侵入の効果を制限し得る、構成可能なロバスト性エージェントを描く。

【図２】１つ以上のロバスト性エージェントに基づくセキュリティシステムが実装され得る、複数の相互接続された通信ネットワークを有するプロセスまたは工業プラントの例示的なブロック図である。

【図３】分散プロセス制御システム及びプロセス自動化ネットワークの形態の、オペレータ及び保守ワークステーション、サーバ、及びコントローラノードを含む様々なネットワークノードを有する、図２のプラントネットワークのうちの１つの例示的な図であり、その中で図１のロバスト性エージェントを使用するセキュリティシステムが、感染または易感染したノードの効果を制限し、それらを潜在的に検出するように動作する。

【発明を実施するための形態】

【００２０】

一般的に言えば、本明細書に記載されるネットワークセキュリティシステムは、通信ネットワーク上の１つ以上のデバイスに入ってくる、及び／またはそこから出ていくネットワークトラフィックを分析して、メッセージタイプ、送信者、受信者、送信者／受信者の対などの１つ以上のメッセージ特徴に基づいて、全てはネットワークセキュリティを実行する目的で、メッセージが伝達されるべきか、フィルタリングされるべきか、またはさらに処理されるべきかを決定することによって、脅威検出及び脅威修復を実装する。場合によって、さらなる処理は、特定期間内に特定のタイプ（または他の特徴の組）を有するメッセージのボリュームをカウントすること、または検出することを含んでよい。さらなる処理は、伝達されるか、または隔離される（例えば、消去される）かのいずれかである特定タイプの、または他の特徴の組を有するメッセージをもたらし得、及び／またはノードで侵入検出を実行する、デバイスをネットワークから外してネットワークをデバイス内の感染から保護するなどのいくつかの他の措置が講じられ得る。本明細書に記載されるセキュリティシステムは、工業システムまたはプロセス制御ネットワーク構成のプライオリ性質が、特定のネットワーク構成から生じる、予想または既知のトラフィック統計に基づいて、基本的なメッセージトラフィックが分析される（及び比較的既知であり静的となる）のを可能にするため、有効に実行する。すなわち、プロセス制御、工業システム、またはプラント自動化ネットワーク内のネットワーク通信の構成は、一般に、通信ネットワークの実装または動作前にある程度周知であり、故にネットワークトラフィックの基本的な構成は、これらのネットワークの使用または動作中に著しく変化する傾向はない。代わりに、ネットワーク通信トラフィックは、通信ネットワークの動作中に（統計的意味で）比較的静的である傾向があり、故に、ネットワークメッセージまたはメッセージパターンのタイプまたは特徴の変化は、特に統計的な意味において、元の構成または所望の構成の一部でないネットワークへの侵入を示し得る。

【００２１】

一般的に言えば、例えば、イーサネットインターフェースを有する工業制御システムデバイスは、デバイス動作に悪影響を及ぼす可能性がある様々なネットワークトラフィックパターン及び条件に曝される。本明細書に記載されるセキュリティシステムは、ネットワーク上のデバイスへの出入りなどの、ネットワーク上の特定のメッセージトラフィックパターンを規制するルールで構成または更新されることができる。しかしながら、制御シス

テムオペレータは、変則的なトラフィックにもかかわらずロバストであるデバイスを必要とし、故に、本明細書に記載されるセキュリティシステムは、有害なデバイス動作を防ぐためにトラフィックを適切に検出して扱うように動作中に構成されてよい。場合によって、ルールは、動的に構成可能であってよく、ルールは、予測的保護を提供するための条件または他のルールに基づく依存性を有してよく、ルールは、有効なロバスト動作を提供するように他のルールを動的に発動してよく、またルールは、特定のインストールにおいて特定のトラフィックパターンに適合可能であってよい。さらに、本明細書に記載されるセキュリティシステムは、ネットワークが動作可能である間に、動的に発見された有害なトラフィックパターン及び／または条件から保護するためのルールを自動的に作成することができる。なおもさらに、場合によって、セキュリティシステムは、それらのデバイスから出る出口トラフィックを分析し、許可されたトラフィックルールまたはメッセージタイプに一致しない変則的なトラフィックを破棄することによって、易感染された制御システムデバイスまたはノードからの攻撃を特定して防ぐことができ、それにより、悪意のあるネットワーク攻撃を開始する制御システムでのこれらのデバイスの使用を防ぐ。

【００２２】

より具体的に、本明細書に記載されるセキュリティシステムは、セキュリティが行われる通信ネットワークの１つ以上のノードに位置する構成可能なロバスト性エージェントを含む。一般的な意味において、構成可能なロバスト性エージェントは、ある特定の既定の特徴を有する特定のタイプ、流れ、またはパターンのメッセージの存在が、ノード内で動作する（もしくはいくつかの他のノードでは、そのノードを攻撃する）マルウェアを示し得るが、またはそうでなければノード上またはノードからの攻撃を示し得るという理論下で、通信ノードに出入りするメッセージトラフィックの流れを管理（例えば、制限）するように動作する。ロバスト性エージェントは、ノードに流入するか、またはノードから流出するメッセージのそれぞれを分析して、メッセージが、（１）予想される、（２）予想されない、または（３）ある程度予想されるが、制限されたボリュームもしくはレベルに限られる、特徴を有するかどうかを決定することによって、そのような攻撃の効果を制限するように動作する。着信メッセージが、ネットワーク通信内で予想される特徴（例えば、メッセージタイプ、ある特定の送信者もしくは受信者、または送信者／受信者の対など）の組を有する場合、ロバスト性エージェントは、単にメッセージを伝達することができる（メッセージがネットワークからの着信メッセージであるときはノード内に、またはメッセージがノードからの発信メッセージであるときはネットワークリンク上に）。着信メッセージが、受信または送信デバイスでのネットワーク通信で予想されない特徴（例えば、メッセージタイプ、ある特定の送信者もしくは受信者、または送信者／受信者の対など）の組を有する場合、ロバスト性エージェントは、メッセージがノード内のより高レベルの通信スタックに到達すること（メッセージがネットワークからの着信メッセージであるとき）、またはネットワークリンク上に配置されることを防ぐように、メッセージを削除、フィルタリング、または隔離してよい。着信メッセージが、ネットワーク通信内である程度予想されるが、制限されたレベルまたはボリュームに限られる特徴（例えば、メッセージタイプ、ある特定の送信者もしくは受信者、または送信者／受信者の対など）の組を有する場合、ロバスト性エージェントは、そのタイプの、またはその特徴の組を有するメッセージをカウントして、ある特定の期間にわたってロバスト性エージェントを通過する、そのタイプの、またはその特徴の組を有するメッセージの数を決定することができる。

【００２３】

この場合、ロバスト性エージェントは、ボリュームが特定レベルよりも低い場合、メッセージを伝達し得、ボリュームが特定レベルまたは閾値を超える場合は、メッセージをブロックまたは隔離し得る。さらに、ボリュームが特定レベルを超え、ノードが攻撃下にあるか、またはマルウェアもしくはネットワークを攻撃している感染を有することを示す場合、ロバスト性エージェントは、さらなる措置を講じて通信ネットワークを保護し得る。例えば、ロバスト性エージェントは、そのノードが特定タイプのいくつかのメッセージをネットワーク上に送信しているときに、ロバスト性エージェントが位置するノードを切断

してもよい。代替として、ロバスト性エージェントが別のノードからの攻撃を検出したとき（他のノードからの疑わしいメッセージの数またはボリュームに基づいて）、ロバスト性エージェントは、信号またはメッセージを他のノードに（例えば、通信ネットワーク上で）送信して、他のノード自体をネットワークから切断させることができる。これらまたは他の場合、ロバスト性エージェントは、ユーザまたはオペレータに潜在的な攻撃及び攻撃の詳細の一部を通知し得るか、ネットワークの１つ以上のノードでマルウェアまたは侵入検出アプリケーションを起動して、これらのノードにウイルス、マルウェア、または他の侵入があるかどうかを決定し得るか、または任意の他の所望の措置を講じ得る。

【００２４】

所望される場合、ロバスト性エージェントは、ロバスト性エージェントが、それが位置する特定のネットワーク環境、それが位置する特定のノードなどにおいて、より良好に適合されるのを可能にするように構成可能であり得る。具体的に、ロバスト性エージェントは、特定のノードに出入りする予想されるメッセージトラフィックに基づいて構成可能であり得、これはノードのタイプ（例えば、コントローラノード、ユーザインターフェースノード、データベースノードなど）に基づいて、ノードの場所などに基づいて変更され得るか、または異なり得る。さらに、ロバスト性エージェントの構成可能な性質は、ノードでのメッセージトラフィックの検出された統計に基づいて、または通信システムの１つ以上のノードの構成の変化に応答するなどして、より良好に動作する（例えば、構成される）のを可能にし得る。

【００２５】

図１は、上記の機能を実行するために通信ネットワーク内で使用され得る、例示のロバスト性エージェントまたはモジュール１０を示す。具体的に、ロバスト性モジュール１０は、ネットワークノードのインターフェース（例えば、ネットワークデバイス）及びネットワークリンク１２の物理層に配設される。より具体的に、ロバスト性モジュール１０は、ネットワークリンク１２に接続されるイーサネットドライバ１４などのネットワークドライバと、ネットワークデバイスのネットワーク通信スタック１６の高次層との間に結合され得る。図１に示されるように、ロバスト性モジュール１０は、インバウンド構文フィルターモジュール２０、及びドライバ１４とネットワークスタック１６との間に結合されたインバウンドボリュームフィルターモジュール２２を含み、ネットワークリンク１２からネットワークデバイスに送信されるメッセージを処理することができる。ロバスト性モジュール１０は、アウトバウンド構文フィルターモジュール３０、及びネットワークスタック１６とドライバ１４との間に結合されたアウトバウンドボリュームフィルターモジュール３２を含み、ネットワークデバイス（ネットワーク通信スタック１６）からネットワークリンク１２に送信されるメッセージを処理することもできる。ロバスト性モジュール１０はまた、モジュール２０、２２、３０、及び３２のそれぞれに接続された破棄されたメッセージロギングブロック４０、モジュール２０、２２、３０、及び３２のうちの１つ以上によって実装され得る構成ルール（例えば、ロジックルール）を記憶するルールメモリ４２、ならびにルールメモリ４２においてルールを構築（例えば、確立または変更）するために使用され得るルールビルダーブロック４４も含む。なおもさらに、ロバスト性モジュール１０は、ボリュームフィルター２２または３２のうちの一方が、相当量の特定タイプの（例えば、特定の特徴の組を有する）メッセージを検出したときに、アラートをユーザに提供するように動作し得るアラートジェネレータ４６を含んでよい。アラートジェネレータ４６はさらにまたは代わりに、ネットワークのこのデバイスもしくは異なるノードでマルウェアもしくはウイルス検出ソフトウェアを起動する、デバイスをネットワークから切断する、またはネットワークの別のノードにあるロバスト性エージェントにメッセージを送信して、そのノードが自らをネットワークから切断させるなどの他のアクションを実行することができる。

【００２６】

動作中、メッセージは、通信リンク１２から受信され、ドライバ１４で処理されて、例えば、リンク１２上のメッセージのそれぞれが、特定のネットワークデバイスに、または

そのデバイス内もしくはそれと関連付けられたアドレスもしくはアプリケーションにアドレス指定されたかを決定する。当然のことながら、ドライバ１４は、図１に示されるイーサネットドライバなどの任意の既知または所望のタイプのネットワークドライバであり得、任意の既知の方法で動作することができる。その後、ネットワークデバイスに向けられたメッセージは、これらのメッセージを分析して、メッセージの１つ以上の特徴を決定する、インバウンド構文フィルターモジュール２０の入力４９に伝達される。これらの特徴は、メッセージのタイプ（例えば、ＵＤＰ、ＴＣＰなど）、メッセージと関連付けられた送信者及び／または受信者、メッセージの長さ、パリティ、セキュリティタイプ、メッセージの優先度、メッセージを送信もしくは受信するポート、または任意の他の所望のメッセージ特徴を含んでもよい。これらの１つ以上のメッセージ特徴は、一般に、ヘッダー及び／もしくはトレーラー、またはメッセージの他の隠蔽部分の情報に見出され得るか、またはそれから決定され得るが、メッセージのペイロードまたはデータ部分の特徴が、フィルタリングのために審査され、使用されてもよい。

【００２７】

一般的に言うと、インバウンド構文フィルターモジュール２０は、各メッセージの１つ以上の特徴の組を決定する（この特徴の組は、ルールメモリ４２に記憶され得るか、もしくはそれによって提供され得るか、または構文モジュールフィルター２０にハードコードされ得る）。メッセージと関連付けられた１つ以上の特徴の組を決定した後、次に構文フィルターモジュール２０は、これらの決定された特徴に基づいて動作する１つ以上のロジックルールを適用して、このメッセージをさらに処理する方法を決定する。具体的に、決定されたメッセージ特徴及びルールメモリ４２内のルールに基づいて、構文フィルターモジュール２０は、メッセージ（安全または予想されるメッセージであるとみなされる）を出力５０から直接ロバスト性モジュール１０の出力に、故にネットワークデバイスのネットワーク通信スタック１６の次の層上に伝達することができ、メッセージがデコードされ、処理されて、ネットワークデバイス内の適切な受信者に任意の標準方法で伝達される。他の場合、決定されたメッセージ特徴及びルールメモリ４２内のルールに基づいて、構文フィルターモジュール２０は、メッセージ（安全でない、またはネットワーク内で明らかに許可されていないとみなされる）を出力５２から破棄されたトラフィックロギングブロック４０に伝達され得、これがこのメッセージ、このメッセージに関するメタデータ、またはネットワーク侵入を分析する際、ルールメモリ４２内のルールを変更して、より良好またはより正確なフィルタリングを実行する際などに今後使用するためのメッセージに関する他の情報をログすることができる。さらに他の場合、決定されたメッセージ特徴及びルールメモリ４２内のルールに基づいて、構文フィルターモジュール２０は、メッセージ（潜在的に安全でないとみなされる）をインバウンドボリュームフィルターモジュール２２の出力５４から入力５５に伝達してもよい。

【００２８】

一般的に言えば、これらのメッセージは、あるタイプであり得るか、または正当なネットワークトラフィックで使用され、また典型的なマルウェアまたはウイルスによってシステムを特にボリュームで攻撃するために使用される特徴を有し得るため、インバウンドボリュームフィルターモジュール２２は、これらのメッセージが、必ずしもそうではないが、正当であり得ることを示す特徴を有するメッセージを扱う。インバウンドボリュームフィルターモジュール２２は、これらのメッセージを受信し（インバウンド構文フィルターモジュール２０によって検出される）、これらのメッセージを（１つ以上のカウンターを使用して）カウントして、追加として、特定期間にわたって、または過去の特定期間にわたって、そのようなメッセージがいくつ受信されたかを記録し得る。故に、インバウンドボリュームフィルターモジュール２２は、ある特定のメッセージ特徴の組を有するメッセージのメッセージトラフィックのボリューム（例えば、特定期間にわたる、または特定期間内のメッセージの数）を決定する。当然のことながら、インバウンドボリュームフィルターモジュール２２は、任意の数の異なるメッセージ特徴の組に対してメッセージボリュームを追跡することができる。

【００２９】
いずれにしても、あるメッセージタイプ（すなわち、特定の特徴の組を有するメッセージ）の現在のボリュームが既定の閾値よりも低い場合（閾値はルールメモリ４２に記憶され得る）、インバウンドボリュームフィルターモジュール２２は、ネットワークデバイス内で処理するために、出力５６を介してスタック１６にメッセージを伝達することができる。反対に、あるメッセージタイプ（すなわち、特定の特徴の組を有するメッセージ）の現在のボリュームが既定の閾値を超える場合（閾値はルールメモリ４２に記憶され得る）、インバウンドボリュームフィルターモジュール２２は、例えば、出力５７を介して破棄されたトラフィックロギングブロック４０にメッセージを提供することによって、メッセージをブロックまたは破棄することができる。ここでも同様に、ブロック４０は、メッセージ及び／またはメッセージに関するメタデータをログして、これらのブロックされたメッセージに関する統計を決定することができる。なおもさらに、インバウンドボリュームフィルターモジュール２２は、あるメッセージタイプの現在のボリュームを、複数の閾値と比較し得るか、または複数の閾値を使用して、講じられる措置を決定し得る。例えば、メッセージがボリュームフィルターモジュール２２で受信され、このタイプのメッセージの現在検出されたボリュームが、第１の（例えば、より低い）閾値よりも低い場合、ボリュームフィルターモジュール２２は、このメッセージをネットワークデバイスのスタック１６に伝達し得る。しかしながら、メッセージがボリュームフィルターモジュール２２で受信され、このタイプのメッセージの現在の検出されたボリュームが、第１の（例えば、より低い）閾値よりも大きいが、第２の（例えば、より高い）閾値よりも低い場合、ボリュームフィルターモジュール２２は、メッセージをロギングブロック４０に送信することによってメッセージをブロックし得る。しかしながら、メッセージがボリュームフィルターモジュール２２で受信され、このタイプのメッセージの現在の検出されたボリュームが、第２の（例えば、より高い）閾値よりも高い場合、ボリュームフィルターモジュール２２は、メッセージをブロックし得（メッセージをロギングブロック４０に送信することによって）、ネットワークを保護するためにいくつかのさらなる措置を実行することもできる。例えば、第２以上のボリューム閾値が伝達されたとき、ボリュームフィルター２２は、ネットワークデバイス上の潜在的な攻撃を示すアラートをユーザに送信し得る、アラートジェネレータ４６と通信することができ、ネットワークデバイスをネットワークリンク１２から切断して、デバイスを攻撃から保護することができ、メッセージを送信するデバイスなどの別のデバイスにメッセージを送信して、ネットワークを保護するためにそのデバイス自体をネットワークから切断させることができ、デバイス内でマルウェアまたはウイルス検出ソフトウェアを起動することができる。当然のことながら、アラートジェネレータ４６を提供するか、またはネットワーク内で異なる措置を取らせるために、任意の数の異なるボリュームレベル閾値が確立されてよい。

【００３０】
図１に示されるように、ロバスト性モジュール１０は、アウトバウンド構文フィルターモジュール３０及びアウトバウンドボリュームフィルターモジュール３２によって定義されたアウトバウンドフィルタリングパスも含む。この場合、モジュール３０及び３２が、ネットワークリンク１２を介して別のデバイスに送信される、通信スタック１６から受信された発信メッセージ上で動作することを除いて、アウトバウンド構文フィルターモジュール３０は、インバウンド構文フィルターモジュール２０と同様に動作し、アウトバウンドボリュームフィルターモジュール３２は、インバウンドボリュームフィルターモジュール２２と同様に動作する。さらに、モジュール３０及び３２は、それぞれモジュール２０及び２２によって使用されるものと同じルールを使用し得るが、モジュール３０及び３２は、インバウンドメッセージに適用されるものとは異なるアウトバウンドメッセージ上のフィルタリング動作を許可するように異なるルールを使用し得る。故に、モジュール３０及び３２は、インバウンドメッセージ上で動作するモジュール２０及び２２に関して上記のものと本質的に同じ方法で、アウトバウンドメッセージ上で一緒に動作し、それにより、ロバスト性モジュール１０が位置するノードまたはデバイス内に常駐する潜在的なマル

ウェア及び感染からネットワーク上の他のデバイスを保護する。したがって、アウトバウンドモジュール３０及び３２は、ロバスト性エージェント１０と関連付けられたデバイス内に常駐するマルウェア、ウイルス、または他のソースの存在を検出するように動作することができ、また例えば、ボリュームフィルター３２が、既定レベルまたはボリュームの、特定タイプまたは構成のアウトバウンドメッセージがデバイスから送信されるのを検出したときに、アラートジェネレータ４６と通信して、アラートジェネレータにアラートをユーザに送信させる、及び／またはそのデバイスをネットワークから切断させるように動作することができる。

【００３１】

動作中、ロギングブロック４０は、破棄されたメッセージを受信、分析、及び追跡するように動作し得る。具体的に、ロギングブロック４０は、破棄されたメッセージのそれぞれに関する、タイミング、送信者／受信者、メッセージのタイプ、メッセージの長さ、構文またはボリュームフィルターモジュールでメッセージが破棄された理由などを含む様々なメタデータを決定することができ、これらのメッセージに対するログを作成し得る。ブロック４０は、着信及び発信メッセージに対して、各メッセージのタイプに対して、メッセージの各送信者／受信者に対してなど、別個のログを作成することができる。当然のことながら、ロギングブロック４０は、任意の他のタイプのログを作成してもよく、またこれらのログをユーザインターフェース、データベースデバイス、または任意の他のデバイスに、要求に応じて、ログがある特定の長さになると定期的に、または任意の他の所望のトリガー事象に応答して送信し得る。なおもさらに、ロギングブロック４０は、そのように所望される場合、予め構成された、及びハードコードされたルールに基づいて、またはルールリスト４２からのルールに基づいて、情報をログする、及び／または破棄されたメッセージに関するログ情報を送信することができる。このように、破棄されたメッセージのロギングも同様に構成され得る。ロギングブロック４２は、そのように所望される場合、ネットワークリンク１２上でログをエクスポートし得るか、またはローカル接続などのロバスト性モジュール１０への任意の他の通信接続を介してログをエクスポートし得る。

【００３２】

同様に、上で示されるように、構成可能なルールリスト４２は、インバウンド構文フィルターモジュール２０、インバウンドボリュームフィルターモジュール２２、アウトバウンド構文フィルターモジュール３０、アウトバウンドボリュームフィルターモジュール３２、ロギングブロック４０、及び変更ジェネレータ４６のそれぞれに対するルールを記憶することができる。これらのルールは、別のアプリケーションと通信し得る（ネットワークリンク１２を介して、またはブルートゥース接続、無線インターネット接続、携帯デバイスからの断続的ハードワイヤ接続などのロバスト性モジュール１０への任意の他の通信接続を介して）ルールビルダーモジュール４４を介して構成可能であり、ルールリスト４２に記憶されたルールを構築するために使用される１つ以上のルールを受信することができる。他のアプリケーションは、ネットワークリンク１２上のユーザインターフェース（例えば、構成インターフェース）に記憶される、または例えば、ハードワイヤもしくは無線通信接続など）を介してモジュール１０に断続的に接続する形態デバイスに記憶されるルールビルダーアプリケーションであってよい。所望される場合、ルールビルダー４４は、モジュール１０に対する通信インターフェースであり得、ルールリスト４２に記憶されたルールのオンラインまたは動作中構成を可能にし、それにより、ロバスト性モジュール１０がネットワーク上の新しい構成、メッセージトラフィックの統計の変更などに照らして再構成されるのを可能にする。しかしながら、所望される場合、ルールビルダー４４は、デバイスに内在し得るか、またはロバスト性モジュール１０が位置するデバイスのインターフェース（例えば、ＵＳＢポートもしくは他の外部メモリポート）にプラグインされ得る書き込み保護されたフラッシュメモリであり得る。そのようなフラッシュメモリは、使用中に書き込み可能でないため、フラッシュメモリ上に記憶されたルールを変更することができず、これがロバスト性モジュール１０をルールリスト４２の変更を介して感染され得ることから保護する。すなわち、ルールリスト４２を変更するために、フラッシュメモ

リ４４は、除去され、ロバスト性モジュール１０内で使用するために、その上に新しいルールで置き換えられる必要がある。ルールリスト４２のこの構成がロバスト性モジュール１０を侵入からより安全にする一方で、システムを動作中に構成しにくくもする。当然のことながら、所望される場合、ルールメモリ４２は、ルールビルダー４４と同じモジュールに組み込まれ得る。ある場合では、ルールリスト４２内のルールのうちのいくつかは、フラッシュメモリに記憶され得、故に構成可能でないが、これらのルールは、動作中に変更することができるルールリスト４２などのメモリに記憶されたリストを使用することができ、それにより、ロバスト性モジュール１０のいくらかの動作中構成を許可する。単なる例示の目的で、下の表１は、ロバスト性モジュールのインバウンド及びアウトバウンド構文及びボリュームフィルターのそれぞれに使用され得る例示のルールの組を提供する。表１は、各ルールに対して、そのルールがフラッシュメモリに記憶されているかどうか、ルールが構成可能であるかどうか、ルールがＷｉｎｄｏｗｓオペレーティングシステム実装を使用するかどうか、及びルールがネットワーク内の組み込みデバイス（例えば、コントローラ）において使用されるかどうかも定義する。当然のことながら、表１は、特定のロバスト性モジュール１０において使用され得るルールの組の１つの実施例のみを提供し、任意の他のタイプ及び数のルールが、任意の特定のロバスト性モジュール１０で使用され得る。

【表１】

ルール記述	フラッシュイン？	構成可能？	Ｗｉｎｄｏｗｓ？	組み込み？
構文インバウンドフィルター				
特定のポートを狙った全てのパケットを破棄する（例えば、ＵＤＰポート１９９へのパケットを破棄する）。	はい	はい*（例えば、新しいＵＤＰポートは、破棄されたインバウンドポートトラフィックリストに含まれ得る）	はい	はい
無効な長さを有する全てのパケットを破棄する（例えば、ＩＰヘッダーの長さがＴＣＰパケットに対して短すぎる場合）。	はい	いいえ	いいえ	はい
技術的に有効な長さであるが、制御ネットワーク環境に対して予想される長さに含まれないパケットを破棄する（例えば、プロトコルによって指定された最小ＵＤＰ長を超えるが、制御トラフィックの予想される長さよりも短い／長いＵＤＰパケットを破棄する）。このルールは、ＩＰアドレス範囲及びポートによってさらに定義され得る。	はい	はい	はい－ネットワークＩＰアドレス範囲及びポートを制御するように制限され得る	はい
ボリュームインバウンドフィルター				
ある期間内に過剰なパケットが受信された後、特定タイプのパケットを単一ソースから破棄する（例えば、ＴＣＰ　ＳＹＮ）。	はい	はい*（例えば、新しいソースＩＰは、別個の破棄ポートトラフィックリストに含まれ得る）	はい	はい
最大パケット破棄制限に到達した後に全てのパケットを破棄する。この破棄制限に対してカウントするパケットのタイプは、構成可能であり得る（例えば、Ｂｏｇｕｓ　ＴＣＰ　ＳＹＮ、ＴＣＰ　ＵＲＧ）。	はい	はい	はい	はい

【表２】

特定期間内に過剰なパケットが受信された後にパケットを破棄する（例えば、ＴＣＰ　ＵＲＧ）。	はい	はい*（例えば、パケットカウント制限は、特定のパケットタイプに対して調整され得る）	はい	はい
予想される最大レベルを超えるＵＤＰトラフィックのパケット速度制限を行う。速度制限は、構成可能であり得る。	はい	はい	はい	はい
構文アウトバウンドフィルター				
データが通常はその上で、またはそれを通って通信しないポートに送信されるパケットを破棄する。	はい	はい*（例えば、新しいポートは、別個の破棄アウトバウンドポートトラフィックリストに含まれ得る）	はい	はい
無効な長さを持つパケットを破棄する（例えば、ＩＰヘッダーの長さは、ＴＣＰパケットには短すぎる）	はい	いいえ	いいえ	はい
技術的に有効な長さであるが、制御環境に対して予想される長さに含まれず、デバイス／システム上で何らかのエラー動作を示すパケットを破棄する（例えば、プロトコルによって特定された最小ＵＤＰ長を超えるが、コントローラプロトコルトラフィックの予想される長さよりも短い／長いＵＤＰパケットを破棄する）。このルールは、ＩＰアドレス範囲及びポートによってさらに定義され得る。	はい	はい	はいーネットワークＩＰアドレス範囲及びポートを制御するように制限される	はい
アウトバウンドトラフィックを既知のネットワークサブネットＩＰアドレス範囲に制限する（例えば、ＩＰアドレス８．８．８．８及び８．８．４．４に向かう任意のトラフィックをブロックする）。	はい	はい	はい	はい

【表３】

ボリュームアウトバウンドフィルター				
予想されるＴＣＰトラフィックの量に応じて、ある特定の量が特定の時間の長さまたは期間内に受信された後、アウトバウンドＴＣＰＳＹＮを破棄する。	はい	はい*（例えば、構成可能なパラメータは、一般に、ボリューム制限を含み、特定のパケット署名に対するマッチングがオン／オフにされ得る）	いいえ	はい
ＩＣＭＰピンのように、典型的に使用されない過剰なパケットを破棄する	はい	はい*（例えば、構成可能なパラメータは、一般に、ボリューム制限を含むか、またはルールの組に含まれ得る新しいパケット署名を含む）	はい	はい
構成可能な閾値を超える過剰な最大長ＵＤＰパケットを破棄する。	はい	はい	はい	はい

表１

【００３３】

単なる実施例として、図２及び３は、図１のロバスト性モジュール１０のうちの１つ以上で作製されたネットワークセキュリティシステムが、インストールされて使用され得る、例示のプラントネットワークを示す。具体的に、図２は、それぞれが様々なネットワークノードを有する、異なるが相互接続されたいくつかの通信ネットワーク１１２、１１４、１１６、及び１１８を含むプラントまたは工業通信システム１１０を示す。図２の通信ネットワーク１１２は、例えば、イーサネットバスまたは任意の他の有線もしくは無線通信バスもしくはネットワークであり得る、通信バス１２４によって相互接続された複数のノード１２２Ａ～１２２Ｈを含むビジネス通信ネットワークであってよい。ノード１２２Ａ、１２２Ｂは、例えば、ビジネスアプリケーションまたはプログラムが実行するコンピュータ、サーバ、ワークステーションなどを含んでよく、またノード１２２Ｃは、例えば、ビジネスデータ、工業プラント構成データ、またはプラントに関する任意の他の所望のデータを記憶するデータベースであってよい。同様に、ノード１２２Ｄ、１２２Ｅ、及び１２２Ｆは、ネットワーク１１２を他の通信ネットワーク１１４、１１６、１１８にそれぞれ接続して、ネットワーク間通信を許可するゲートウェイノードであり得る。なおもさらに、ノード１２２Ｇは、ネットワーク１１２をインターネット、クラウド、または他の広域ネットワークに接続して、ネットワーク１１２が遠隔サーバ、プラント、または他のコンピュータと通信するのを可能にするゲートウェイノードであり得る。

【００３４】

この例では、ネットワーク１１４、１１６、及び１１８は、有線または無線通信バスまたはネットワークリンクによって相互接続された様々なノードを含む、プラント（プロセスプラントまたは工業プラントなど）制御ネットワークである。プラント制御ネットワー

ク１１４、１１６、１１８のそれぞれは、様々なタイプのデバイスのうちのいずれかをそのノードに含んでよい。例えば、プラント制御ネットワーク１１４及び１１６は、有線通信ネットワークとして示され、それぞれが１つ以上のユーザインターフェースデバイス１３０と、ネットワーク１１４及び１１６に対するプラント制御ネットワーク構成データを記憶し得るデータベースまたはヒストリアン１３２と、この場合はイーサネット通信バスの形態の、通信バス１３６を介して相互接続された１つ以上のプロセスコントローラノード１３４と、１つ以上のサーバまたはプロセッサノード１３８とを含む。プロセス制御ノード１３４は、入力／出力（Ｉ／Ｏ）及びフィールドデバイス（例えば、センサ、バルブ、制御デバイス）などの、１つ以上の有線または無線サブネットワーク１４０を介して他のデバイスに通信可能に結合された１つ以上のプロセスコントローラを含んでよい。サブネットワーク１４０内のフィールドデバイスは、例えば、バルブ、センサ、トランスミッタ、またはプラント内のいくつかのパラメータもしくはプロセス変数を計測するか、またはプラント内の材料動作もしくは材料の流れに関連するいくつかの物理的制御動作を実行する、他の計測もしくは制御デバイスの形態を取り得る。フィールドデバイスサブネットワーク１４０は、例えば、ハイウェイアドレス可能遠隔トランスミッタ（ＨＡＲＴ（登録商標））プロトコル、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスプロトコル、Ｐｒｏｆｉｂｕｓプロトコル、ＣＡＮプロトコルなどの任意の所望のプロセス制御通信プロトコルまたはパラダイムを使用し得る。なおもさらに、フィールドデバイスサブネットワーク１４０は、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）ネットワークなどの有線または無線ネットワークとして実装されてよい。ネットワーク１１４及び１１６は、ネットワーク１１４及び１１６をネットワーク１１２、インターネット、または他のＷＡＮなどに接続するノード１２２Ｄ、１２２Ｅにゲートウェイデバイスを含んでもよい。当然のことながら、これらのゲートウェイデバイスは、ファイアウォール及び他のセキュリティ機構またはアプリケーションを提供することができる。

【００３５】

同様の方法で、通信ネットワーク１１８は、無線イーサネットプロトコル、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコル、ＩＳＡ１００無線プロトコルなどの無線通信プロトコルを使用し得る無線通信ネットワークとして示される。通信ネットワーク１１８は、ユーザインターフェースデバイスまたはワークステーション１３０、データベース１３２、プロセスコントローラ１３４、サーバ１３６、フィールドデバイスサブネットワーク１４０、ゲートウェイデバイス１３９などの様々なデバイスを含むように示される。当然のことながら、任意の数のこれらのタイプ及び他のタイプのデバイスは、通信ネットワーク１１４、１１６、及び１１８の様々なノードに位置し得る。ネットワーク１１２、１１４、１１６、及び１１８内のネットワークデバイスのうちのいずれかまたは全てが、図１のロバスト性モジュール１０と関連付けられる、及び本明細書に記載されるモジュールのうちのいずれかを含む、様々なソフトウェアモジュールが記憶されて実行され得る、１つ以上のコンピュータ可読メモリ及びプロセッサを含んでよいことが理解されるであろう。

【００３６】

重要なことに、本明細書に記載されるセキュリティシステムは、図２のネットワーク１１２、１１４、１１６、及び１１８のうちのいずれか及び全てにおいて実装され、例えば、マルウェアまたはこれらのネットワークの様々なノード内で実行する他の不正アプリケーションの形態の、これらのネットワークへの侵入の効果を制限することができる。一般的に言えば、ネットワーク１１２、１１４、１１６、及び１１８のそれぞれに対する、またはさらにはネットワーク１１２、１１４、１１６、１１８のうちのいずれかにあるノードのそれぞれに対する別個のロバスト性モジュールに基づくセキュリティシステムが存在し得る。一方で、場合によって、単一セキュリティシステムを使用して、ネットワーク１１４及び１１６、またはネットワーク１１２及び１１４などのネットワーク１１２～１１８のうちの複数をカバーしてもよい。

【００３７】

実施例として、図２のネットワーク１１４、１１６、及び１１８に概して示されるよう

に、ロバスト性モジュールに基づくセキュリティシステムは、これらの各ネットワークのノードのそれぞれのインターフェース（例えば、通信スタック内）及びこれらのネットワークが取り付けられる通信リンクに位置するロバスト性モジュール２１０を含む。ここで、ロバスト性モジュール２１０（本明細書では、トランジットトラフィック分析エージェントとも称される）は、図１のロバスト性モジュールまたはエージェント１０として上述される形態であってよい。追加として、図２は、各ネットワークの各ノードでのロバスト性モジュールを示すが、必ずしも保護されるネットワークの各ノードに別個のロバスト性モジュールを提供する必要がないこともある。代わりに、本明細書に記載されるセキュリティは、ネットワークの各ノードに位置するロバスト性モジュールを有する必要なしに、ネットワーク内で１つ以上のロバスト性モジュールを使用することができる。例えば、セキュリティシステムは、ユーザインターフェースデバイスなどのより複雑なデバイスにロバスト性モジュール２１０を有することなく、コントローラなどのネットワークの組み込みデバイスのネットワークインターフェースにロバスト性モジュール２１０を含んでよい。いずれにしても、ロバスト性モジュール２１０は、ネットワーク内の任意の所望のデバイスにおいて、任意の所望の方法でインストールされることができ、これらのロバスト性モジュールを使用するセキュリティシステムは、本明細書において具体的に説明される実施例に限定されない。さらに、セキュリティシステムは、ネットワーク１１２、１１４、１１６、及び１１８のノードのうちの１つ以上に位置する構成及びユーザインターフェースサポートモジュール２１１を含んでよい。ユーザインターフェースサポート及び構成アプリケーション２１１は、コンピュータ可読メモリ内に記憶され、これらのデバイスのプロセッサ上で実行して、ロバスト性モジュール２１０のうちのいずれかのルールリスト４２内のルールを構成する能力をユーザに提供し、保護されるネットワークのロバスト性モジュール２１０のうちのいずれかまたは全ての破棄されたトラフィックログをユーザが見るのを可能にしてよく、どのデバイスまたはノードがオフラインで実行されるか、または多量の疑わしいメッセージトラフィックを送信または受信することに関して現在疑わしいかをユーザが把握できるようにしてよく、ユーザがより良好な、または強化されたセキュリティを提供するようにロバスト性モジュール２１０のうちのいずれかを構成するのを可能にする環境を提供してもよい。

【００３８】

一般的に言えば、ロバスト性モジュール２１０のそれぞれは、モジュール内のルールにより、インバウンド及びアウトバウンドメッセージを見るか、または分析して、メッセージを伝達すること、疑わしいメッセージをブロックすること、及び／またはメッセージ上でボリュームフィルタリングをカウントして実行するのを許可する。ロバスト性モジュール２１０は、独立して動作し得るか、または特定のネットワーク内もしくはさらにはネットワークにわたって、調整されたメッセージフィルタリングを提供するように調整され得る。

【００３９】

さらなる実施例として、図３は、図２の通信ネットワーク１１４をより詳細に示す。この実施例において、通信ネットワーク１１４は、ゲートウェイデバイス（例えば、他のネットワーク２２６へのゲートウェイ、外部システム２２８へのゲートウェイ、例えば、インターネット）、もう１つのユーザインターフェースデバイスまたはワークステーション２３０、構成データベース２３２、サーバ２３３、及び２つのプロセス制御ノード２３４Ａ及び２３４Ｂなどの様々なデバイスを相互接続する１つ以上のスイッチ２０２を含み得る、有線イーサネットバス２００を含む。ここで、第１のプロセス制御ノード２３４Ａは、入力／出力（Ｉ／Ｏ）カード２３６及び２３８を介して有線フィールドデバイス２１５～２２２に通信可能に接続され、無線ゲートウェイ２３５及びネットワークバックボーン２００を介して無線フィールドデバイス２４０～２５８に通信可能に接続された１つ以上の冗長プロセスコントローラ２６０を含む。この場合、無線ゲートウェイ２３５は、ネットワーク１１４の第２の制御ノード２３４Ｂである。しかしながら、別の実施形態では、ノード２３４Ａにあるコントローラ２６０は、バックボーン２００以外の通信ネットワー

クを使用して、例えば、別の有線または無線通信リンクまたはＩ／Ｏモジュールを使用することによって、無線ゲートウェイ２３５に通信可能に接続され得る。

【００４０】

例として、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔによって販売されているＤｅｌｔａＶ（商標）コントローラであり得るコントローラ２６０は、フィールドデバイス２１５～２２２及び２４０～２５８のうちの少なくともいくつかを使用して、１つ以上のバッチプロセスまたは連続プロセス、保守アプリケーション、安全システムアプリケーションなどを実装するように動作し得る。コントローラ２６０は、例えば、標準４～２０ｍａデバイスプロトコル、及び／またはＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスプロトコル、ＨＡＲＴ（登録商標）プロトコル、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコルなどの任意のスマート通信プロトコルと関連付けられた任意の所望のハードウェア及びソフトウェアを使用して、フィールドデバイス２１５～２２２及び２４０～２５８に通信可能に接続され得る。コントローラ２６０は、追加として、または代替として、入力／出力（Ｉ／Ｏ）カード２３６、２３８を介して、フィールドデバイス２１５～２２２及び２４０～２５８のうちの少なくともいくつかと他のタイプの接続を介して通信可能に接続されてよい。図３に示されるネットワーク１１４において、コントローラ２６０、フィールドデバイス２１５～２２２、及びＩ／Ｏカード２３６、２３８は、有線デバイスであり、フィールドデバイス２４０～２５８は、無線フィールドデバイスである。当然のことながら、有線フィールドデバイス２１５～２２２及び無線フィールドデバイス２４０～２５８は、任意の他の所望の標準（複数可）またはプロトコル、例えば、今後開発される任意の標準またはプロトコルを含む、任意の有線または無線プロトコルに準拠し得る。

【００４１】

図３のコントローラ２６０は、制御ループを含み得る、１つ以上のプロセス制御ルーチン（メモリ２７２に記憶される）を実装または管理するプロセッサ２７０を含む。プロセッサ２７０は、制御活動または保守、モニタリング、及び安全システム活動などの他の活動を実行するために、フィールドデバイス２１５～２２２及び２４０～２５８、ならびにネットワークバックボーンまたはリンク２００に通信可能に接続された他のノードと通信し得る。制御ルーチンまたはモジュールのうちのいずれかが、そのように所望される場合、異なるコントローラまたは他のデバイスによってその部分を実装または実行させ得ることに留意すべきである。同様に、プロセス制御システム内で実装される制御ルーチンまたはモジュールは、ソフトウェア、ファームウェア、ハードウェアなどを含む任意の形態を取り得る。制御ルーチンは、例えば、オブジェクト指向のプログラミング、ラダーロジック、シーケンシャル機能チャート、機能ブロックダイヤグラムを使用するか、または任意の他のソフトウェアプログラミング言語またはデザインパラダイムを使用して、任意の所望のソフトウェアフォーマットで実装され得る。制御ルーチンは、ランダムアクセスメモリ（ＲＡＭ）または読み出し専用メモリ（ＲＯＭ）などの任意の所望のタイプのメモリに記憶されてよい。同様に、制御ルーチンは、例えば、１つ以上のＥＰＲＯＭ、ＥＥＰＲＯＭ、特定用途向け集積回路（ＡＳＩＣ）、または任意の他のハードウェアもしくはファームウェア素子にハードコードされ得る。故に、コントローラ２６０は、任意の所望の方法で制御戦略または制御ルーチンを実装するように構成され得る。

【００４２】

いくつかの実施形態では、コントローラ２６０は、一般に機能ブロックと称されるものを使用して制御戦略を実装し、各機能ブロックが、オブジェクトまたは制御ルーチン全体の他の部分（例えば、サブルーチン）であり、他の機能ブロックと共に（リンクと呼ばれる通信を介して）動作して、プロセス制御システム内でプロセス制御ループを実装する。制御ベースの機能ブロックは、典型的に、トランスミッタ、センサ、または他のプロセスパラメータ計測デバイスと関連付けられるものなどの入力機能、比例積分導関数（ＰＩＤ）、ファジーロジックなどの制御を実行する制御ルーチンと関連付けられるものなどの制御機能、制御、またはバルブなどのいくつかのデバイスの動作を制御して、プロセス制御

システム内のいくつかの物理的機能を実行する出力機能のうちの１つを実行する。当然のことながら、ハイブリッド及び他のタイプの機能ブロックが存在する。機能ブロックは、コントローラ２６０に記憶され、それによって実行され得るか（典型的に、これらの機能ブロックが標準４～２０ｍａデバイス及びＨＡＲＴデバイスなどのいくつかのタイプのスマートフィールドデバイスに使用されるか、もしくはそれと関連付けられる場合である）、またはフィールドデバイス自体に記憶され、それによって実装され得る（フィールドバスデバイスを用いる場合であり得る）。コントローラ２６０は、１つ以上の制御ループを実装し得る１つ以上の制御ルーチン２８０を含んでよい。各制御ループは、典型的に、制御モジュールと称され、機能ブロックのうちの１つ以上を実行することによって実行されてよい。

【００４３】

有線フィールドデバイス２１５～２２２は、センサ、バルブ、トランスミッタ、ポジショナなどの任意のタイプのデバイスであり得るが、Ｉ／Ｏカード２３６及び２３８は、任意の所望の通信またはコントローラプロトコルに準拠する任意のタイプのＩ／Ｏデバイスであり得る。図３に示される実施形態では、フィールドデバイス２１５～２１８は、アナログラインまたは組み合わされたアナログ及びデジタルライン上でＩ／Ｏカード２２６に通信する標準４～２０ｍａデバイスまたはＨＡＲＴデバイスであるが、フィールドデバイス２１９～２２２は、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバス通信プロトコルを使用してデジタルバス上でＩ／Ｏカード２３８に通信するＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスフィールドデバイスなどのスマートデバイスである。しかしながら、いくつかの実施形態では、有線フィールドデバイス２１５～２２２のうちの少なくともいくつか及び／またはＩ／Ｏカード２３６、２３８のうちの少なくともいくつかは、ビッグデータネットワークを使用してコントローラ２６０と通信し得る。いくつかの実施形態では、有線フィールドデバイス２１５～２２２のうちの少なくともいくつか及び／またはＩ／Ｏカード２３６、２３８のうちの少なくともいくつかは、プロセス制御システムネットワーク１１４のノードであり得る。

【００４４】

図３に示される実施形態では、無線フィールドデバイス２４０～２５８は、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコルなどの無線プロトコルを使用して、無線ネットワーク２９０内で通信する。そのような無線フィールドデバイス２４０～２５８は、無線で通信するようにも構成される（例えば、無線プロトコルを使用して）、ネットワーク１１４の１つ以上の他のノードと直接通信し得る。無線で通信するように構成されていない１つ以上の他のノードと通信するために、無線フィールドデバイス２４０～２５８は、通信バックボーン２００または別の制御通信ネットワークに接続された無線ゲートウェイ２３５を利用してよい。いくつかの実施形態では、無線フィールドデバイス２４０～２５８のうちの少なくともいくつかは、プロセス制御システムネットワーク１１４のノードであってよい。

【００４５】

無線ゲートウェイ２３５は、無線デバイス２４０～２５８、有線デバイス２１５～２２２、及び／またはプロセス制御ネットワーク１１４の他のノードの間の通信結合を提供する。無線ゲートウェイ２３５は、場合によって、有線及び無線プロトコルスタック（例えば、アドレス会話、ルーティング、パケット分割、優先度付けなど）の下位層においてルーティング、バッファリング、及びタイミングサービスを使用する一方で、有線及び無線プロトコルスタックの１つまたは複数の共有層をトンネリングすることによって、通信結合を提供する。他の場合、無線ゲートウェイ２３５は、いかなるプロトコル層も共有しない有線プロトコルと無線プロトコルとの間のコマンドを翻訳し得る。プロトコル及びコマンド会話に加えて、無線ゲートウェイ２３５は、無線ネットワーク２９０内で実装される無線プロトコルと関連付けられたスケジューリングスキームのタイムスロット及びスーパーフレーム（均等に時間間隔で区切られた通信タイムスロットの組）によって使用される同期クロックを提供し得る。さらに、無線ゲートウェイ２３５は、無線ネットワーク２９

０に対するネットワーク管理、及びリソース管理、性能調整、ネットワーク障害の軽減、モニタリングトラフィック、セキュリティなどの管理機能を提供し得る。

【００４６】

有線フィールドデバイス２１５～２２２と同様に、無線ネットワーク２９０の無線フィールドデバイス２４０～２５８は、プロセスプラント内で物理的制御機能を実行することができ、例えば、弁を開閉するか、またはプロセスパラメータの計測を行うか、または他の機能を実行する。しかしながら、無線フィールドデバイス２４０～２５８は、ネットワーク２９０の無線プロトコルを使用して通信するように構成される。そのようにして、無線フィールドデバイス２４０～２５８、無線ゲートウェイ２３５、及び無線ネットワーク２９０の他の無線ノードは、典型的に、無線通信パケットの生成者及び消費者である。

【００４７】

いくつかのシナリオでは、無線ネットワーク２９０は、非無線デバイスを含んでよい。例えば、図３のフィールドデバイス２４８は、旧来の４～２０ｍＡデバイスであってよく、フィールドデバイス２５０は、伝統的な有線ＨＡＲＴデバイスであってよい。ネットワーク２９０内で通信するために、フィールドデバイス２４８及び２５０は、無線アダプタ（ＷＡ）２５２ａまたは２５２ｂを介して無線通信ネットワーク２９０に接続されてよい。追加として、無線アダプタ２５２ａ、２５２ｂは、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバス、ＰＲＯＦＩＢＵＳ、ＤｅｖｉｃｅＮｅｔなどの他の通信プロトコルを支持し得る。さらに、無線ネットワーク２９０は、無線ゲートウェイ２３５と有線通信している別個の物理デバイスであり得る、１つ以上のネットワークアクセスポイント２５５ａ、２５５ｂを含み得るか、または無線ゲートウェイ２３５内で一体型デバイスとして提供され得る。無線ネットワーク２９０は、無線通信ネットワーク２９０内の１つの無線デバイスから別の無線デバイスにパケットを転送するために１つ以上のルータ２５８を含んでもよい。無線デバイス２４０～２５８は、図３において点線によって示される無線通信ネットワーク２９０の無線リンク上で相互に、及び無線ゲートウェイ２３５と通信し得る。

【００４８】

図３のネットワーク１１４は、有限数のフィールドデバイス２１５～２２２及び２４０～２５８と共に、単一コントローラ２６０を示しているに過ぎないが、これは、単に例示的かつ非限定的な実施形態である。任意の数のコントローラは、ネットワーク１１４上に含まれてよく、コントローラ２６０は、任意の数の有線または無線フィールドデバイス２１５～２２２、２４０～２５８と通信して、例えば、プラント内のプロセスを制御することができる。さらに、プロセスプラントは、任意の数の無線ゲートウェイ２３５、ルータ２５８、アクセスポイント２５５、及び無線プロセス制御通信ネットワーク２９０を含んでもよい。

【００４９】

一般的に言えば、セキュリティシステムは、図１に関して記載されるように構成された１つ以上のロバスト性モジュールを使用して、任意の所望の方法でネットワーク１１４内にインストールまたは実装され得る。具体的に、図３に示されるように、セキュリティシステムは、ネットワークノード２２６、２２８、２３０、２３２、２３３、２３４Ａ、及び２３４Ｂのそれぞれ、ならびにスイッチ２０２またはネットワーク１１４の他のエンドポイントデバイスのうちのいずれかに配設されたロバスト性モジュール２１０を含む。図３では完全に詳細に示されていないが、ロバスト性モジュール２１０は、サブノードデバイスのうちのいずれかにおいて、例えば、Ｉ／Ｏデバイス２３６及び２３８において、有線フィールドデバイス２１５～２２２のうちの１つ以上において、または無線デバイス２４０～２５８のうちの１つ以上においてインストールされ得る。図３では、サブノードデバイス内のロバスト性モジュール２１０のそれぞれは、参照番号２１０ａでラベル表示され、それがネットワーク１１４のより大きなノードのサブノード内にあることを示す。図１に関して示されるように、ロバスト性モジュール２１０及び２１０ａは、ノードのそれぞれに出入りするトラフィックを分析し、またフィルタリングを実行してトラフィックに関するメタデータをコンパイルし得る一方で、メッセージ及びボリュームフィルタリング

を実行する。

【００５０】

この例示のセキュリティシステムでは、ロバスト性モジュール２１０は、独立して動作し得るが、相互に通信して、例えば、ボリュームフィルターによって決定されるように、それらのデバイスが多くの疑わしいメッセージを送信している場合、それらそれぞれのデバイスをネットワークから切断するか、または破棄したメッセージログを相互に、またはユーザインターフェースモジュール２１１（ユーザインターフェースデバイス２３０内にあるように示される）を提供するように相互に指示することができる。なおもさらに、ユーザは、ユーザインターフェースモジュール２１１を使用して、ロバスト性モジュール２１０のうちの１つ以上を構成してもよく、ユーザは、それを行うための適切なセキュリティＩＤまたはセキュリティ許可を有する必要があり得る。当然のことながら、ユーザインターフェースモジュール２１１は、１つ以上のネットワークリンク２００上で通信してよく、ユーザインターフェースモジュール２１１は、ネットワーク１１４上の他のコンピュータデバイスのうちのいずれかにおいて、例えば、構成データベース２３２、ゲートウェイデバイス２２６、２２８、スイッチ２０２などにおいてネットワーク上でインストールされてもよい。追加として、フィールドデバイス２１５～２２２、Ｉ／Ｏデバイス２３６、２３８、及び無線フィールドデバイス２４０～２５８などのサブネットワークデバイスからの通信（アラート及び破棄ログなど）は、コントローラ２６０またはゲートウェイデバイス２３５などの主ネットワークノードデバイスに送信されてよく、その後、これらのデバイスは、それらの通信をユーザインターフェースモジュール２１１または他のロバスト性モジュール２１０に転送し得る。なおもさらに、図３に示されるように、構成データベース２３２は、ネットワーク内の構成変更を検出することができ、またこれらの構成変更に基づくロバスト性モジュールルールの組を、ロバスト性モジュール２１０に任意の所望の方法で通信することができる、構成変更モジュール３７０を含む。図３のノードのうちの少なくともいくつかに示されるように、ノードデバイスのそれぞれは、プロセッサ３０９を含み、これはマイクロプロセッサ、ＡＳＩＣ、または様々なロバスト性モジュール２１０を実装及び実行し、プロセッサ３０９上で実行するための、これらのモジュールを記憶するコンピュータ可読記憶３１１を含む、他のプロセッサであり得る。

【００５１】

一般的な意味において、ロバスト性モジュール２１０のルールメモリ４２に記憶されたメッセージ分析ルールは、ネットワーク１１４のノードに出入りするメッセージトラフィックの予想されるまたは正常な動作を反映する。より具体的に、ルールデータベース４２に記憶されたルールは、特定期間中に、例えば、ネットワークが起動して実行しているが、それがセットアップされた直後であるとき、ネットワークが易感染されていないことが比較的確実であるときなど、ネットワーク１１４のノードから来るメッセージまたはトラフィックメタデータを収集して分析することによって生成されてよい。この期間中、生成または収集されたメッセージトラフィックデータは、統計的な意味で、ネットワークの「正常な」または「予想される」動作を反映する。様々なトラフィックパターンパラメータまたは統計は、この期間中に収集されたメッセージトラフィックデータから収集または生成されることができ、このデータは、様々なロバスト性モジュール２１０に対する１つ以上のルールの組を作成する際に使用するために、トラフィックパターンデータベースに記憶されてよい。収集または生成され、またデータベースに記憶されるトラフィックパターンパラメータは、例えば、任意の粒度の任意の特定ノードまたはノードのグループにおけるトラフィックの統計的尺度を含んでよい。すなわち、記憶されたトラフィックパターンパラメータは、任意のタイプのデータ、タイムフレーム、ノードもしくはグループノード、着信もしくは発信、送信者受信、長さなどに関してグループ化または実行されたデータの任意の統計的尺度（例えば、平均、標準偏差、平均、中央値、カウントなど）を示してよく、ネットワークの構成階層を反映する階層などの任意の所望の階層に記憶され得る。トラフィックパターンパラメータは、ノードまたはノードのグループに出入りする通信の任意のタイプまたはグループに対する範囲または制限を含んでもよく、それを超えるとき

、ボリュームフィルター閾値、警告メッセージ、ネットワークからの切断などを反映するか、または引き起こす。これらの範囲または制限は、例えば、固定数の形態の絶対的な制限であり得るか、または第１もしくは第２標準偏差内に含まれる平均値の３倍、中央値もしくは平均値を超える、もしくは下回る既定量などの他の統計的尺度に基づくか、または関連する相対的な制限であり得る。

【００５２】

理解されるように、ルールデータベース４２内のルールが作成され、現在の、または収集されたメッセージを分析してネットワーク内の異常または侵入を検出すべき方法を定義するために使用される。より具体的に、ルールデータベース４２内のルールは、例えば、収集されたメタデータまたは収集されたメッセージに関する統計を、トラフィックパターンデータと比較することによって、及び／またはトラフィックパターン制限もしくは範囲を使用することによって、収集されたメッセージトラフィックを分析すべき方法を特定する。一般的な意味において、図１のフィルターモジュール２０、２２、３０、３２は、ルールデータベース４２に記憶されたルールを実装して、収集されたメッセージデータまたはメタデータを、既知の、所望の、または予想されるトラフィックパターンパラメータと比較する。

【００５３】

同様に、図１に示されるように、ロバスト性モジュール１０は、モジュール２０、２２、３０、及び３２によって実行された分析の結果に基づいて１つ以上のアラート、アラーム、またはメッセージを生成し得る、アラートジェネレータ４６を含んでよい。アラートジェネレータ４６によって作成されたアラート、アラーム、またはメッセージは、ネットワークリンクを介するか、またはその目的で提供されるか、もしくは使用される任意の他の通信リンクを介するかのいずれかで、オペレータ、セキュリティ人員、ＩＴ人員などの任意の所望の人員に送信されてよい。実施例として、アラート、アラーム、またはメッセージは、指定された人の電子メールアカウントに、プラントに関する他のデータも示すオペレータまたはセキュリティーインターフェースに送信されてよく、私有もしくは公共ネットワークを介して指定された人または人の集団に、電話、またはモバイルデバイスなどの任意の所望のデバイスで送達されるテキストメッセージとして送信されてもよい。同様に、これらのアラート、アラーム、またはメッセージは、ネットワークへの潜在的な侵入に応答し、調査する責任がある任意の指定された者の電話、時計、装着可能なデバイス、ラップトップ、タブレットコンピュータなどの携帯デバイス上でアラームまたは通知を発信することができる。場合によって、アラームまたはアラートジェネレータ４６は、感染したまたは潜在的に感染したノードへのアクセスを制限するように動作することができ、ノードをシャットダウンし得るか、または非常に深刻な状況では、通信ネットワーク自体を他のネットワークからシャットダウンもしくは隔離して、侵入によりプラントもしくはプラント内のサブシステムに対して及ぼされる損傷を制限することができる。当然のことながら、アラートジェネレータ４６は、ネットワーク内の他のデバイスと通信して、そのような自動動作をもたらし得るソフトウェアまたはロジックを含んでよい。場合によって、アラートジェネレータ４６は、プラントネットワーク内でそのような自動的措置を講じる前に、例えば、ユーザインターフェースモジュール２１１を介して、ユーザからの許可を求めることができるが、他の場合では、侵入または潜在的な侵入をユーザに通知する前または同時に、ネットワーク内で措置を実行することができる。さらに、自動的措置を講じるとき、アラートジェネレータ４６は、感染した、または潜在的に感染したノードと通信して、そのノードから（出入りする）通信を制限すること、例えば、そのノードからの特定タイプのメッセージを制限または停止すること、そのノードでの特定アプリケーションの動作（異常なメッセージトラフィックを生成し得る）を停止または制限すること、デバイスのある特定のポートを介する通信を停止または制限することなどができる。故に、１つのロバスト性モジュール１０または２１０のアラートジェネレータ４６は、別のロバスト性モジュールのルールメモリ４２のルールを変更または改変して、まず後者のロバスト性モジュールが疑わしいメッセージをリンク上で送信するのを防ぐのを助けることがで

きる。代わりに、または追加として、アラートジェネレータ４６は、他のネットワークに接続されたゲートウェイノードなどの他のノードと通信して、ネットワークと他のネットワークとの間のメッセージを制限または停止することができる。この措置は、重要な動作（例えば、制御動作）がネットワーク上で起こるのを許可し得る一方で、ネットワークを外部ソースから隔離して、少なくとも一時的に、変則的なメッセージトラフィックがネットワークに出入りするのを防ぎ、これがデータ窃盗を制限することができ、ネットワーク内のウイルスが他のネットワークに感染するのを停止することができ、感染したノードを介したネットワークへのさらなる侵入を停止することができる。例えば、アラートジェネレータ４６は、サイト上のセキュリティ人員によって変則が確認されるまで、外部ビジネスシステムと影響される工業制御システムネットワークとの間の全通信を切断し得る。当然のことながら、アラートジェネレータ４６は、セキュリティシステムなどの他のシステムに結合され（通信接続され）、これらの機能を実行することができる。

【００５４】

ルールデータベース４２は、メッセージトラフィックもしくはトラフィックパターン内に変則があるかどうかを決定するために、故にアラートもしくはアラームを生成すべきか、または他のフィルタリングを行うべきかを決定するために、通信ネットワークノードからもしくは通信リンクから受信されたメッセージトラフィックもしくはメッセージメタデータ上で実行される分析を定義する、１人以上のセキュリティ人員、構成人員、ユーザ、オペレータなどによって作成または生成された任意の所望のルールの組を記憶することができる。故に、モジュール２０、２２、３０、及び３２によって用いられるルールは、ノードから収集されたメッセージデータを、そのノードに対する標準またはベースラインのデータの組と比較して、制限または差分変数などの他のトラフィックパターンパラメータによって定義されるように、それらの間に有意差があるかどうかを決定するように動作することができる。

【００５５】

任意の所望のタイプのデータが、メッセージに対してロバスト性モジュール１０及び２１０で入手されて分析され得ること、ならびにルールデータベース４２内のルールが、任意の所望の方法でデータを分析するために作成され得ることが理解されるであろう。例えば、メッセージデータは、メッセージ自体に関する一般的な情報、例えば、ペイロードタイプ、長さ、ソース（構成ノード対非構成ノード、ソースポートなど）、アドレス（ソース及び宛先アドレス、ポートなど）、スコープ（ユニキャスト、マルチキャスト、ブロードキャストなど）、ペイロードタイプ（ＴＣＰ、ＵＤＰ、その他など）、及びタイミング（１日の時間、相対時間、試行率など）；通信情報、例えば、メッセージタイミング（例えば、割合、１日の時間、シーケンスエラーなど）、セキュリティエラー（失敗した統合性、認証、または復号化など）、メッセージコンテンツ（サイズ、フォーマットエラーなど）；ならびに偽情報、例えば、レート制限情報（状態、方法、レート制限など）、及び接続試行（アウトオブシーケンス、不正、スイープなど）を含み得る。当然のことながら、任意の他のタイプのメッセージデータまたはメタデータは、ルール４２内で同様に、または代わりに入手され、使用されてよく、本明細書に提供されるリストが包括的でないことが理解されるであろう。

【００５６】

さらに、メッセージデータは、ネットワークまたはノード内の他の要因またはパラメータ、例えば、送信または受信ノードの役割（例えば、これらのノードがワークステーション、サーバ、ゲートウェイ、コントローラ、Ｉ／Ｏサーバ、リモート端末ユニット（ＲＴＵ）などであるかどうか）に基づいて収集され、記憶され得る。故に、メッセージ及びトラフィックメタデータが、ネットワークの様々な異なる階層レベルで、またはそれに対して、デバイスもしくはノードベース、デバイスもしくはノードロールベース、メッセージベースなどで、またはネットワークの任意の他の階層レベルに対して作成され得ることが理解されるであろう。なおもさらに、制御または通信ネットワークの構成情報を使用して、メッセージメタデータを分析するために、最初にルールを作成するか、もしくは修正す

るか、またはメッセージメタデータ分析を組織化してもよい。一般的に言えば、ネットワークに対する構成情報は、ノード（デバイス）のそれぞれにおけるアプリケーションの数、モジュール、制御ルーチンなど、及びこれらの様々な論理要素、ソフトウェア要素、及びハードウェア要素が相互に通信する方法に関する情報を含み、通信ペア（送信者／受信者ペア）、通信タイミング、頻度、メッセージのタイプ、制御システムの役割またはデバイスタイプなどが挙げられる。この構成情報を使用して、ノードのうちのいずれかでメッセージを分析するために使用されるルールを作成または修正することができる。すなわち、構成階層情報（例えば、どのデバイス及びモジュールがネットワーク内のどの他のモジュール及びデバイスに関連しているか）を含む構成情報を使用して、メッセージを分析するためのルールのパラメータを作成、修正、または記入することができる。実施例として、構成情報を使用して、例えば、メッセージを分析するために、一般化されたルールのサブセット（すなわち、プロファイル）を選択することができる。構成情報を使用して、１つ以上の一般化されたルールパラメータ内の特定の値にプラグインすることもでき（例えば、ルールが＜購読者＞のプレースホルダを有する場合、構成情報を使用して、その構成に列挙される特定の購読者に関するアドレス及びポート情報を記入することができる）。この方法で、有効なロジックルールは、デバイスまたはノードの制御システム構成に基づいて、より大きな一般ルールの組から特定ルールのサブセットに調整され得る。

【００５７】

なおもさらに、図２及び３に示されるように、セキュリティシステムは、例えば、ネットワーク構成データベースまたはサーバデバイス１２２Ｃもしくは２３２に記憶され得るネットワーク構成変更モジュール３７０を含んでよい。一般的に言えば、構成変更モジュール３７０は、通信ネットワークに対するネットワーク構成の変更を検出するように動作し、その後、これらの変更及び／またはこれらの変更の通知を、例えば、ネットワークリンクを介してユーザインターフェースモジュール２１１に送信する。本明細書で使用される場合、構成変更は、ネットワーク上のデバイスまたはデバイスの組の動作に対して行われた任意の変更を含んでよく、新しいデバイス、アプリケーション、モジュールなどの追加、任意のデバイス、アプリケーション、モジュールなどの削除、ならびにデバイス、アプリケーション、モジュールなど、パラメータ、設定、または他の構成の変更（任意のハードウェア、ソフトウェア、またはファームウェア設定の変更を含む）を含み、例えばバッチプロセスなどで使用される、例えばレシピを変更するなどの、通信及びプロセス制御設定を変更することを含む。この場合、構成エンジニアまたは他のユーザが、例えば、新しいアプリケーション、またはモジュールをネットワークに追加すること、ネットワーク内のアプリケーションまたはモジュールが相互に通信する方法を変更することなどによってネットワーク構成を変更したときはいつも、ネットワーク構成変更モジュール３７０は、そのような変更を検出し、通知をユーザインターフェースモジュール２１１に送信して、ユーザにネットワーク構成の変更を知らせる。当然のことながら、変更モジュール３７０は、構成データベース（例えば、図３のデータベース２３２）に位置するように示されているが、構成モジュール３７０は、構成アプリケーションへのアクセスを有するか、またはそれを実装する（ネットワークの構成を変更するか、もしくはユーザが変更するのを可能にする）、または他の方法で構成の変更が通知される任意のデバイスまたはコンピュータであり得、任意の所望の方法で動作して、ネットワーク構成の変更を検出することができる。

【００５８】

いずれにしても、ネットワークの構成に対して変更が行われたときはいつも（例えば、ネットワーク上の、またはネットワークに結び付けられたデバイスのうちのいずれかにおいて、任意のソフトウェア、機能ブロック、モジュールなどの通信アスペクトの追加、削除、または変更をもたらす）、変更検出モジュール３７０は、ユーザインターフェースモジュール２１１に通知を送信して、ネットワークトラフィックパターンまたは詳細の変更または潜在的な変更をユーザに知らせることができる。この通知は、ユーザが新しいルールを作成するか、またはロバスト性モジュール２１０のうちの１つ以上に既にあるルール

を改変し、それにより、新しいネットワーク構成に照らして、ロバスト性モジュール２１０をより良好に構成するのを可能にし得る。

【００５９】

故に、理解されるように、ネットワーク構成の変更は、例えば、ある特定タイプのネットワークメッセージを増加または減少させることによって、ネットワークメッセージの流れを変更することができ、特定タイプのネットワーク通信を（例えば、ネットワーク上の様々なデバイス間、またはネットワークのノードにある様々なデバイス内で実行されるアプリケーション間の特定タイプの通信の特性または量を変更することによって）変更する。状況によって、新しい構成の結果として、１つ以上のロバスト性モジュール２１０のルールデータベース４２内のルールを変更、追加、または削除して、ルールデータベースの１つ以上のルール内でプロファイルプラグインを実装して、新しい構成のパラメータに一致させるか、または反映させるなどによって、例えば、ルールを新しい構成に調整することが望ましい場合がある。例えば、新しいタイプの通信は、新しい構成によって追加されてよく、ルールは、新しい通信に基づいてプロファイルプラグインで更新されてよく、またその後、このルールを使用して、これらの新しいタイプの通信と関連付けられたメッセージを分析してもよい。

【００６０】

さらに、本明細書に記載されるセキュリティシステムは、別個の構文及びボリュームフィルターを有するように示されているが、単一フィルターが、これらの異なるフィルターのそれぞれについて記載される機能を実行することができる。例えば、単一フィルタリングモジュールは、ネットワークデバイスのプロセッサ上で実行され、デバイスのルールメモリに記憶されたロジックルールを使用して、１つ以上の第１のメッセージ特徴の組を有するメッセージを伝達すること、１つ以上の第２のメッセージ特徴の組を停止すること、及び１つ以上の第３のメッセージ特徴の組を有するメッセージをカウントすることができ、またさらに、１つ以上の第３のメッセージ特徴の組と関連付けられたカウントに基づいて、１つ以上の第３のメッセージ特徴の組を有するメッセージを伝達または停止するように動作することができる。

【００６１】

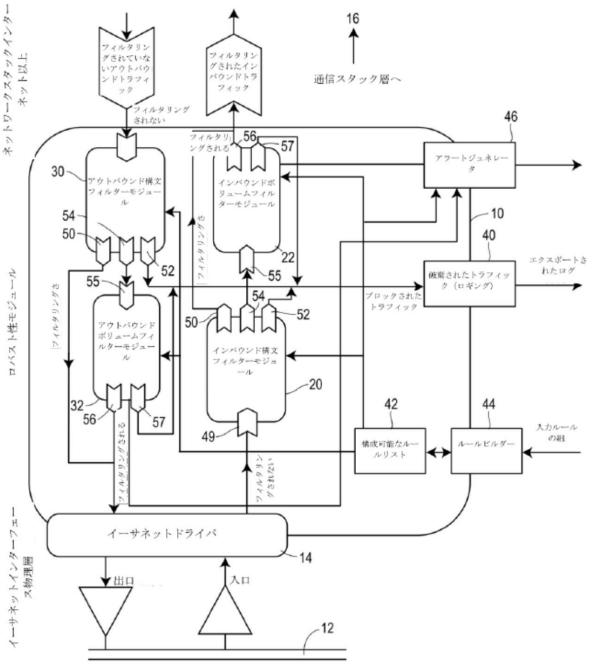
本明細書に記載されるセキュリティ技術は、イーサネット、及びフィールドバス、ＨＡＲＴ、及び標準４～２０ｍａプロトコルなどの様々な既知のプロセス制御プロトコルを使用するネットワークプロセス制御デバイス及びシステムと共に使用されるように記載されたが、本明細書に記載されるセキュリティ技術は、当然のことながら、任意の他のプロセス制御通信プロトコルまたはプログラミング環境を使用する任意のタイプの制御デバイス内で実装されることができ、任意の他のタイプのデバイス、機能ブロック、またはコントローラと共に使用されてよい。本明細書に記載されるセキュリティ特徴は、好ましくは、ソフトウェアで実装されるが、それらは、ハードウェア、ファームウェアなどで実装されてよく、コンピュータデバイスと関連付けられた任意の他のプロセッサによって実行されてもよい。故に、本明細書に記載される方法及びルーチン及びシステムは、そのように所望される場合、標準多用途ＣＰＵ内、または例えば、ＡＳＩＣなどの特異的に指定されたハードウェアまたはファームウェア上で実装され得る。ソフトウェアで実装されるとき、このソフトウェアは、任意のコンピュータ可読メモリ内、例えば、コンピュータもしくはプロセッサのＲＡＭまたはＲＯＭ内の磁気ディスク、レーザディスク、光ディスク、または他の記憶媒体上などに記憶され得る。同様に、このソフトウェアは、例えば、コンピュータ可読ディスクまたは他の輸送可能なコンピュータ記憶機構上を含む、任意の既知のまたは所望の送達方法を介して、ユーザまたはプロセス制御システムに送達され得るか、または電話線、インターネットなどの通信チャネル上で変調され得る。

【００６２】

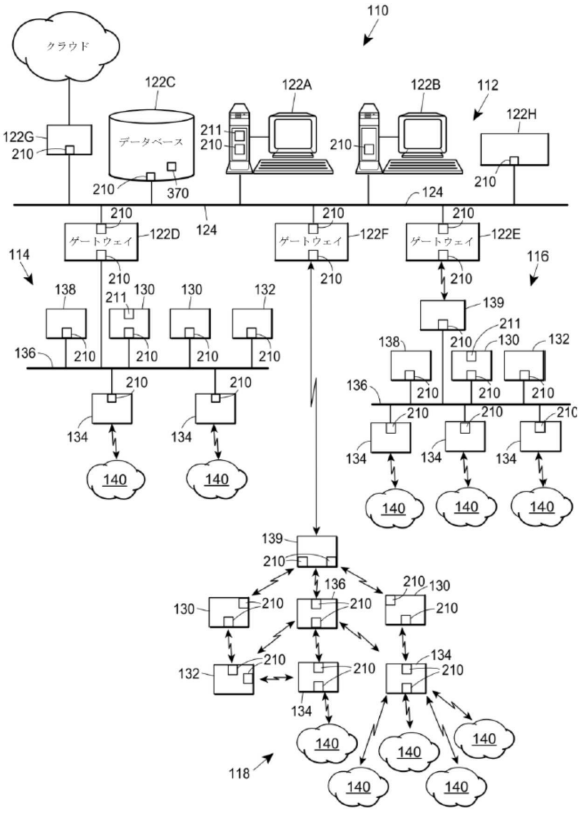
さらに、本発明は、特定の実施例を参照して説明されたが、これは単なる例示であり、本発明を制限するものではないことが意図され、本発明の趣旨及び範囲から逸脱することなく、開示される実施形態に対して変更、追加、または削除が行われてよいことが当業者

には明らかとなるであろう。

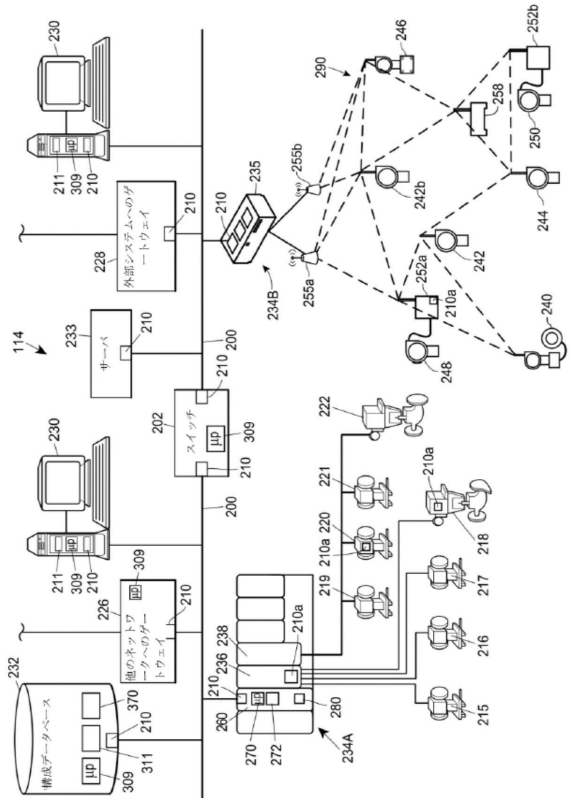
【図１】



【図２】



【図３】


114
200
202
210
211
212
214
215
216
217
218
219
220
221
222
226
228
230
232
233
234A
234B
235
238
240
242
242b
244
246
248
250
252a
252b
255a
255b
258
260
270
272
280
290
309
311
370
スイッチ
サーバ
外部システムへのゲートウェイ
他のネットワークへのゲートウェイ
構成データベース

フロントページの続き

(72)発明者 ヴィナヤ エス. レイアペタ
アメリカ合衆国 ７８６１３ テキサス州 シダー パーク コナー メイソン コープ ４５００
(72)発明者 ヤコブ ビー. レスチャンスキー
アメリカ合衆国 ７８７５３ テキサス州 オースティン ノース ラマー ブールバード １２００７ ナンバー３２６
(72)発明者 ウィリアム イー. ベネット
アメリカ合衆国 ７８６２８ テキサス州 ジョージタウン ヴァル ヴァルデ ドライブ ４２０３

審査官 羽岡 さやか

(56)参考文献 特開２００６－０６０３０６（ＪＰ，Ａ）
特開２００８－２７８３５７（ＪＰ，Ａ）
特開２０１４－１２３９９６（ＪＰ，Ａ）
特表２０１４－５１９１１３（ＪＰ，Ａ）
特開２００４－１８５６２２（ＪＰ，Ａ）
特開２００５－２２９５７３（ＪＰ，Ａ）
渡辺 哲仁，ＩＴで進化する設計機器の監視保守システム，富士時報，富士電機株式会社，２００３年 7月１０日，P.429(65)-433(69)
織田 薫，パケット・フィルタリングでより安全に ルーターの設定で実現 不要なパケットは遮断，日経Ｉｎｔｅｒｎｅｔ Ｓｏｌｕｔｉｏｎｓ 第６５号，日経ＢＰ社 Nikkei Business Publications,Inc.，２００２年１１月２２日，P.124-131
高木 淳史 Atsushi TAKAGI，内容と数量に基づくパケット選択プロセッサの実現と評価 Implementation and Evaluation of Packet Selection Processor Based on Packet Quantity and Contents，電子情報通信学会技術研究報告 Ｖｏｌ．１０４ Ｎｏ．６５９ IEICE Technical Report，日本，社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers，２００５年 2月１１日，第104巻，P.65-70

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－１２／９５５
Ｇ０５Ｂ ２３／０２
Ｇ０６Ｆ ２１／５５