

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6496522号
(P6496522)

(45) 発行日 平成31年4月3日(2019.4.3)

(24) 登録日 平成31年3月15日(2019.3.15)

(51) Int.Cl.

H04L 12/70 (2013.01)

F 1

H04L 12/70

D

請求項の数 19 外国語出願 (全 16 頁)

(21) 出願番号 特願2014-219873 (P2014-219873)
 (22) 出願日 平成26年10月29日 (2014.10.29)
 (65) 公開番号 特開2015-91129 (P2015-91129A)
 (43) 公開日 平成27年5月11日 (2015.5.11)
 審査請求日 平成29年10月23日 (2017.10.23)
 (31) 優先権主張番号 14/072,425
 (32) 優先日 平成25年11月5日 (2013.11.5)
 (33) 優先権主張国 米国(US)

(73) 特許権者 390041542
 ゼネラル・エレクトリック・カンパニー
 アメリカ合衆国、ニューヨーク州 123
 45、スケネクタディ、リバーロード、1
 番
 (74) 代理人 100137545
 弁理士 荒川 智志
 (74) 代理人 100105588
 弁理士 小倉 博
 (74) 代理人 100129779
 弁理士 黒川 俊久
 (74) 代理人 100113974
 弁理士 田中 拓人

最終頁に続く

(54) 【発明の名称】安全なファイル転送のためのシステムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

データを転送するための方法(500)であって、
 インバウンド接続を防止するファイアウォール(108)の背後のオンサイトシステム
 (110)と関連するオンサイトプロセッサにより、転送ディレクトリに前記オンサイト
 システム(110)に配置された資産のオペレーションデータを含む出力ファイルを書
 き込むステップ(520)と、

前記オンサイトプロセッサにより、非同期インテリジェント転送サービスをスケジュー
 リングするステップ(530)と、

前記オンサイトプロセッサにより、前記オンサイトシステム(110)と中央システム
 (120)との間の一方向暗号化リンクに基づいて安全な証明書を確立するステップ(5
 40)と、

前記オンサイトプロセッサにより、中央システム(120)に前記出力ファイルを含む
 メッセージを送信するステップと、

前記中央システム(120)と関連する中央プロセッサにより、前記オンサイトシステム
 (110)からの以前のメッセージに関連する開いているアウトバウンドー方向ポート
 に、前記オンサイトシステム(110)からの前記以前のメッセージに対する応答内でフ
 ァイルダウンロード要求メッセージを送信するステップ(610)であって、前記ポート
 はアウトバウンド以外の通信を防止し応答以外のメッセージをブロックする、送信するス
 テップ(610)と、

10

20

前記オンサイトプロセッサにより、非同期並行並列ファイルダウンロードのためのダウンロードコマンドメッセージを起動するステップ(620)と、

前記オンサイトプロセッサにより、以前に開かれた接続を使用して前記ポートにわたり前記ファイルのうちの少なくとも1つを送信するステップと、
を含む、方法(500)。

【請求項2】

以前に開かれた接続を使用して前記ポートにわたり直列にアウトバウンドデータグラムを送信するステップと、

前記オンサイトシステム(110)により、インバウンドデータグラムを再構成するステップと、

を含む、、請求項1に記載の方法(500)。

10

【請求項3】

前記中央システム(120)により、各アウトバウンドデータグラムおよび少なくとも1つの完全なファイルのチェックサムによって前記アウトバウンドデータグラムのデータトランSPORT信頼度を実行することをさらに備える、請求項1に記載の方法(500)。

【請求項4】

前記オンサイトシステム(110)により、各インバウントデータグラムおよび少なくとも1つの完全なファイルのチェックサムによって前記インバウンドデータグラムのデータトランSPORT信頼度を実行することをさらに備える、請求項2に記載の方法(500)。

20

【請求項5】

前記アウトバウンドデータグラムを送信することは、低帯域幅のサービス(243)を介して前記アウトバウンドデータグラムを送信することを備える、請求項1乃至4のいずれかに記載の方法(500)。

【請求項6】

前記オペレーショナルデータを収集することであって、前記資産に関連づけられた複数のセンサと通信する複数のオンサイトコントローラ(111、113)から前記オペレーショナルデータを収集することを備える、請求項1乃至5のいずれかに記載の方法(500)。

30

【請求項7】

前記ファイアウォール(108)は、標準的な双方向トランSPORT制御プロトコル通信を防止する、請求項1乃至6のいずれかに記載の方法(500)。

【請求項8】

圧縮技法を使用して前記データを管理することをさらに備える、請求項1乃至7のいずれかに記載の方法(500)。

【請求項9】

前記オペレーショナルデータの品質および時間の一貫性を保証することをさらに備える、請求項1乃至8のいずれかに記載の方法(500)。

【請求項10】

40

前記オペレーショナルデータのアナリティクスおよび診断を実行することをさらに備える、請求項1乃至9のいずれかに記載の方法(500)。

【請求項11】

ファイアウォール(108)の背後のオンサイトシステム(110)を備えるデータを転送するためのシステム(100)であって、

前記オンサイトシステム(110)に関連するオンサイトプロセッサが、

前記オンサイトシステム(110)に配置された資産のオペレーショナルデータを収集し、

転送ディレクトリに前記オペレーショナルデータを含む出力ファイルを書き込み、

非同期インテリジェント転送サービスをスケジューリングし、

50

前記オンサイトシステム（110）と中央システム（120）との間の一方向暗号化リンクに基づいて安全な証明書を確立し、

非同期並行並列ファイルアップロードのためのコマンドアップロードメッセージを起動し、

前記オペレーショナルデータを含む、関連づけられたアウトバウンドデータグラムを作成し、

予め決定された特定のポートにわたり前記アウトバウンドデータグラムを送信し、

ここで、前記予め決定された特定のポートは、アウトバウンド以外の通信を防止し応答以外のメッセージをブロックする、

ように動作可能であり、

10

前記中央システム（120）に関連するオンサイトプロセッサが、

受信したアウトバウンドデータグラムに少なくとも部分的に基づいて、前記アウトバウンドデータグラムを再構成し、

開いているアウトバウンド一方向ポートに、前記オンサイトシステム（110）からの以前のメッセージに対する応答内でファイルダウンロード要求メッセージを送信し、

ように動作可能であり、

前記オンサイトシステム（110）に関連するオンサイトプロセッサがさらに、

非同期並行並列ファイルダウンロードのためのダウンロードコマンドメッセージを起動し、

追加のアウトバウンドデータグラムを作成し、

20

以前に開かれた接続を使用して、前記アウトバウンド一方向ポートにわたり直列に前記追加のアウトバウンドデータグラムを送信する

ように動作可能である、

システム（100）。

【請求項12】

前記中央システム（120）がさらに、

各アウトバウンドデータグラムおよび完全なファイルのチェックサムによって前記アウトバウンドデータグラムのデータトランSPORT信頼度を実行する

ように動作可能である、

請求項11に記載のシステム（100）。

30

【請求項13】

前記オンサイトシステム（110）がさらに、

各インバウントデータグラムおよび完全なファイルのチェックサムによって前記インバウンドデータグラムのデータトランSPORT信頼度を実行する

ように動作可能である、請求項11または12に記載のシステム（100）。

【請求項14】

前記オンサイトシステム（110）がさらに、

低帯域幅のサービス（243）を介して前記アウトバウンドデータグラムを送信する
ように動作可能である、請求項11乃至13のいずれかに記載のシステム（100）。

【請求項15】

前記オンサイトシステム（110）がさらに、

前記資産に関連づけられた複数のセンサと通信する複数のオンサイトコントローラ（111、113）から前記オペレーショナルデータを収集する

ように動作可能である、請求項11乃至14のいずれかに記載のシステム（100）。

【請求項16】

前記ファイアウォール（108）は、標準的な双方向トランSPORT制御プロトコル通信を防止するように動作可能である、請求項11乃至15のいずれかに記載のシステム（100）。

【請求項17】

前記オンサイトシステム（110）がさらに、

50

圧縮技法を使用することによって前記データを管理する

ように動作可能である、請求項11乃至16のいずれかに記載のシステム(100)。

【請求項18】

前記オンサイトシステム(110)がさらに、

前記オペレーショナルデータの品質および時間の一貫性を保証する

ように動作可能である、請求項11乃至17のいずれかに記載のシステム(100)。

【請求項19】

前記中央システム(120)が、

前記オペレーショナルデータのアナリティクスおよび診断を実行する

ように動作可能である、請求項11乃至18のいずれかに記載のシステム(100)。 10

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、一般的に、通信セキュリティに関し、特に、安全なファイル転送のためのシステムおよび方法に関する。

【背景技術】

【0002】

監視診断(M&D)センターは、発電所ユニットならびに他の資産のために非常に多くのサービスを提供し得る。そのようなサービスは、資産の監視、イベントの追跡、トリップイベントの報告、根本的原因の分類、強制停止の検出、診断、およびサイトへのさまざまな勧告を伴う報告を含み得る。生のオペレーショナルデータならびに後処理データが、性能および信頼度の調査、保証サポート、および技術研究および開発のためにさまざまな技術チームによって使用され得るアナリティクスから導出され得る。 20

【0003】

しかしながら、相対的に安全なファイル転送を要求する既存の発電所の大きなセットに対し、新たな要求が課せられている。多くのサイトは、北米電力信頼度協議会(NERC)のまたは他の規制上のセキュリティ要求および他の通信セキュリティの難題に適合する必要がある。加えて、これらのサイトの多くは、限られた帯域幅の接続および相対的に不安定なまたはそうでなければ信頼できないリンクを有する。 30

【0004】

典型的には、オンサイト監視が発電所のインフラストラクチャ内に設けられる。オンサイトネットワークは普通、インバウンド接続を防止し得る発電所端のファイアウォールおよびプロキシによって保護されるので、オンサイト監視が非ルータブルであることを強い。さらに、すべての標準的な双方向TCP/HPTP通信ポートは普通、システムのセキュリティを保証するためにファイアウォールによってブロックされる。

【0005】

現在の通信は典型的に、双方向ベースの通信ポートスキーマを要求し、現在のデータトランスポートテクノロジーは一般的に、ダイアルアップのまたは低帯域幅のネットワークトポロジーに適切に対処することができない(たとえば、著しい待ち時間、ストレス条件下での帯域幅の管理)。さらに、一方向汎用ファイル転送ソリューションが利用不可能である。

【発明の概要】

【0006】

新たそしてますます増加する顧客のセキュリティ要求を満たすために、オンサイト監視システムと中央監視診断インフラストラクチャとの間のデータのトランスポートのために安全なデータ転送を提供する、相対的に安全なファイル転送ソリューションが必要とされる。NERCのまたは他の規制上の要求および他の通信セキュリティの難題に適合し得る、限られた帯域幅の接続および相対的に不安定なまたはそうでなければ信頼できないリンクを有するオンサイト監視サイトをサポートするために、安全なファイル転送パッケー 40

ジが開発される必要がある。

【0007】

上記ニーズの一部または全部が、本開示のある特定の実施形態によって対処され得る。例示的な実施形態によると、ファイアウォールの背後のオンサイトシステムによりオペレーショナルデータを収集することと、転送ディレクトリに出力ファイルを書き込むことと、非同期インテリジェント転送サービスをスケジューリングすることと、オンサイトシステムと中央システムとの間の一方向暗号化リンクに基づいて安全な証明書を確立することと、非同期並行並列ファイルアップロードのためのコマンドアップロードメッセージを起動することと、関連づけられたアウトバウンドデータグラムを作成することと、予め決定された特定のポートにわたりアウトバウンドデータグラムを送信することと、中央システムによりアウトバウンドデータグラムを再構成することとを含み得る、データを転送するための方法が開示される。

【0008】

方法はさらに、中央システムにより、開いているアウトバウンド一方向ポートに、オンサイトシステムからの以前のメッセージに対する応答内でファイルダウンロード要求メッセージを送信することと、オンサイトシステムにより、非同期並行並列ファイルダウンロードのためのダウンロードコマンドメッセージを起動することと、中央システムにより、関連づけられた安全なデータグラムを作成することと、以前に開かれた接続を使用して上記ポートにわたり直列にインバウンドデータグラムを送信することと、オンサイトシステムにより、インバウンドデータグラムを再構成することとを含み得る。

【0009】

別の実施形態では、データを転送するためのシステムが開示される。システムは、ファイアウォールの背後のオンサイトシステムを備え得る。オンサイトシステムは、オペレーショナルデータを収集し、転送ディレクトリにファイルを書き込み、非同期インテリジェント転送サービスをスケジューリングし、オンサイトシステムと中央システムとの間の一方向暗号化リンクに基づいて安全な証明書を確立し、非同期並行並列ファイルアップロードのためのコマンドアップロードメッセージを起動し、関連づけられたアウトバウンドデータグラムを作成し、予め決定された特定のポートにわたりアウトバウンドデータグラムを送信するように動作可能であり得る。中央システムは、受信したアウトバウンドデータグラムに少なくとも部分的にに基づいてアウトバウンドデータグラムを再構成し、開いているアウトバウンド一方向ポートにオンサイトシステムからの以前のメッセージに対する応答内でファイルダウンロード要求メッセージを送信するように動作可能であり得る。

【0010】

本開示の他の実施形態、特徴、および態様が、本明細書において詳細に説明され、特許請求される開示の一部とみなされる。他の実施形態、特徴、および態様は、以下の詳細な説明、添付図面、および請求項を参照して理解され得る。

【0011】

ここでは添付図面を参照するが、添付図面は必ずしも正確な縮尺率ではない。

【図面の簡単な説明】

【0012】

【図1】本開示の実施形態に係るオンサイト監視システムと中央監視診断インフラストラクチャとの間のデータのトランスポートのために安全なデータ転送を提供する例示的なシステムアーキテクチャの模式的なブロック図である。

【図2】本開示の実施形態に係る例示的なオンサイト監視システムの模式的なブロック図である。

【図3】本開示の実施形態に係る例示的な中央監視診断インフラストラクチャの模式的なブロック図である。

【図4】本開示の実施形態に係る例示的なオンサイト監視システムの機能ブロック図である。

【図5】本開示の実施形態に係るオンサイト監視システムと中央監視診断インフラストラ

10

20

30

40

50

クチャとの間でのデータの例示的な安全なファイルアップロードを示すフローチャートである。

【図6】本開示の実施形態に係るオンサイト監視システムと中央監視診断インフラストラクチャとの間でのデータの例示的な安全なファイルダウンロードを示すフローチャートである。

【図7】オンサイト監視システムへの例示的な安全なリモートアクセスを示すフローチャートである。

【発明を実施するための形態】

【0013】

本開示の例示的な実施形態がここで、添付図面に関連して以下においてより十分に説明され、添付図面には、全部ではないが一部の実施形態が示される。実際、本開示は、多くの異なる形態で具体化ことができ、本明細書に説明される実施形態に限定されるものと解釈されるべきではなく、むしろこれらの実施形態は、この開示が適用可能な法的要請を満足するように提供される。同一の番号は、全体を通して同一の要素を指す。

10

【0014】

限られた帯域幅の接続または相対的に不安定なまたはそうでなければ信頼できないリンクを有する発電所のオンサイト監視をサポートする安全なファイル転送を達成するために、さまざまなハードウェア、ソフトウェア、およびネットワーキングテクノロジーを組み合わせた新たなインフラストラクチャが開発されている。本開示のある特定の実施形態は、オンサイト監視システム上のリポジトリからの非同期でサービス指向型のデータ抽出を可能にし、アナリティクス処理のために中央ストレージリポジトリにデータを転送する技術的効果を有し得る。本開示のある特定の実施形態の別の技術的効果は、セキュリティ、サービスの動的な保証、および信頼度特徴を提供すると同時に、中央監視診断インフラストラクチャにおける指定されたサーバとオンサイト監視システムとの間でのファイルの非同期並列同時ダウンロードおよびアップロードを可能にし得る。

20

【0015】

図面の図1を参照すると、オンサイト監視システム110と中央監視診断インフラストラクチャとの間のデータのトランスポートのために安全なデータ転送を提供する例示的なシステムアーキテクチャ100の模式的なブロック図が示されている。

【0016】

30

オンサイト監視システム110は、さまざまなネットワーキング能力を有するWindows（登録商標）ベースのプラットフォーム102（典型的にはハイコンピューティングサーバ）を使用することによって実現されることができ、発電所サイトで企業ファイアウォール108の背後に配置され得る。オンサイトネットワーク106は、インバウンド接続を防止する発電所端のファイアウォール108およびプロキシ104によって保護され得るので、オンサイト監視が非ルータブルであることを強いる。さらに、すべての標準的な双方向TCP/HHTTP通信ポートは、ファイアウォール108によってブロックされ得る。

【0017】

オンサイト監視の安全なリモートアクセスソリューションは監視診断ユーザ119、134に、オンサイト監視システム110に安全にかつリモートでアクセスし、ある特定のアドミニストレーションまたはマネジメントタスクを実行する能力を提供し得る。通信セキュリティは、HTTPS/TLSプロトコルスタックをインテリジェントエージェントと呼ばれるカスタマイズされたソフトウェアパッケージと統合することによって提供され得る。

40

【0018】

中央システムインターネット114を利用するユーザ119または外部のインターネット130に接続されたリモートユーザ134は、リモートエンタープライズサーバ118への接続を確立し得る。リモートエンタープライズサーバ118は、エンタープライズトンネリングサーバ116との接続を確立し得る。ユーザ119、134が統いて、オンサ

50

イト監視システム 110へのユーザ起動のリモートデスクトッププロトコル（RDP）セッションを確立し得る。通信セキュリティは、リモートアクセスセッションデータをカプセル化するTLS / SSLベースのトンネリング方法を使用して提供され得る。

【0019】

M & D ユーザ 119またはリモートユーザ 134が、オンサイト監視システム 110へのRDP接続を要求し得る。トラヒックポート 443は一方向である（アウトバウンドのみに開いている）ので、エージェントサーバ 116は、オンサイト監視システム 110内のサーバ上に存在するインテリジェントエージェント 102からの任意の以前のメッセージに対する応答内でRDPセッション要求メッセージを起動し得る。インテリジェントエージェント 102が続いて、オンサイト監視システム内のRDPモジュールに接続し得る。10

。

【0020】

図 2 を参照すると、本開示の実施形態に係るオンサイト監視（OSM）200の例が示されている。OSM 200は、さまざまなネットワーキング能力を有するWindows（登録商標）ベースのプラットフォーム（典型的にはハイパフォーマンスサーバ）上で実現されることができ、発電所サイトで企業ファイアウォールの背後に配置される。

【0021】

データ収集ソフトウェアモジュール 210は、ユニットのオペレーションデータと動的なデータ、たとえば、温度、圧力、流量、クリアランス（たとえば、2つのコンポーネント間の距離）、およびターボ機械類の振動データ、の収集に関連づけられ得る。ネットワーク接続能力および生データ分解能に基づいたさまざまなタイプのコントローラが、ユニットセンサとインターフェース接続するために使用される。コントローラは、専用コントローラ 111から標準的なイーサネット（登録商標）データ収集システム（EDAS）113までの範囲にわたり得る。収集された生データが続いて処理され、データハブを介して他のOSMモジュールに転送され得る。データハブは、膨大な量のリアルタイム生産情報を収集し、より高いレベルの分析アプリケーションへの信頼できる情報の配布のほかに監視の自動化を実行し得る。そのようなデータハブは、W SST 115、CIMPLI C ITY 117、およびE HISTORIAN 119のコレクタモジュールのようなある特定の専用ハブを含み得る。加えて、これらのモジュールは、データ品質および時間の一貫性のために組み合わせられたソースを提供し得る。30

【0022】

ストレージソフトウェアモジュール 220は、データの記憶およびアーカイブに関連づけられ得る。ソフトウェアプラットフォーム 220は、PROFICY HISTORY ANのような専用プラットフォームであり得、時系列データならびにアナリティクス出力によって生成された処理データのローカルストレージのための能力を提供し得る。それはまた、さまざまな圧縮および内挿技法を使用してデータ品質を管理する能力を提供し得る。30

【0023】

データ処理モジュール 230は、データ処理ならびにイベントおよびアラームの段階的拡大に関連づけられ得る。アナリティクスベースのデータ処理が、CENTRAL CONDITION ASSESSMENT PLATFORM - LOCAL EDITION（CCAP - LE）231および連続診断エンジン（CDE）ルールエンジンプラットフォーム 233のような専用プラットフォームによって提供され得る。アラームおよびイベントの段階的拡大は、動作エンジン 235によって実行されることができ、eメールまたはウェブベースのサービスを介して通知を送信され得る。40

【0024】

転送モジュール 240は、中央監視診断システムへのデータ転送に関連づけられ得る。サイトに固有のセキュリティ要求、ネットワークトポロジー、および利用可能な帯域幅に基づいて、2つのタイプのトランSPORTメカニズムが一般的に利用可能である。一つ目のメカニズムは、リアルタイムデータストリーミングトランSPORTを提供するために、50

コレクタサービスにヒストリアンコレクタ 241 を活用し得る。二つ目のメカニズムは、安全（一方向トラヒック／プッシュ）で信頼できる非同期並列ファイルトランSPORTのために、低帯域幅のインテリジェントエージェントモジュール 243 によって提供されるサービスを組み合わせる。

【0025】

したがって、少なくとも 1 つの技術的效果は、低帯域幅のインテリジェントエージェントモジュールに、安全で信頼できる一方向トラヒックの非同期並列ファイルトランSPORTの提供を可能にさせることができる。

【0026】

図 3 は、本開示の実施形態に係る例示的な中央監視診断インフラストラクチャ 300 を示す。10

【0027】

中央システム転送モジュール 310 は、オンサイトシステムからのデータ転送に関連づけられ得る。2つのタイプのトランSPORTメカニズムが一般的に利用可能である。一つ目のメカニズムは、リアルタイムデータストリーミングを提供するために、コレクタサービス 311 にヒストリアンコレクタを活用し得る。二つ目のメカニズムは、相対的に安全（一方向トラヒック／プッシュ）で信頼できる非同期並列ファイルトランSPORTのために、相対的に低い帯域幅のインポートサービス 313 を提供し得る。

【0028】

中央ストレージソフトウェアモジュール 320 は、最初に収集され OSM のフリートから転送された時系列データのデータストレージおよびアーカイブに関連づけられ得る。このソフトウェアプラットフォームは、時系列データだけでなく、アナリティクス出力によって生成された処理データの記憶のための機能を提供し得る。ストレージモジュール 320 は、膨大な量のリアルタイム生産情報をアーカイブし、超高速で配布する、エンタープライズワイドなデータヒストリアンサービスを提供し得る。それはまた、さまざまな圧縮および内挿技法を使用してデータ品質を管理する機能を提供し得る。20

【0029】

PROFICY HISTORIAN のような中央ストレージソフトウェアモジュール 320 は、無数の分析可能性を可能にするために、長年にわたる履歴データをリアルタイムデータと比較するように動作可能であり得る。このソリューションは、機器および処理がどのように実行されているかに対しそれらがどのように実行されるべきかをよりよく理解するために、フリートにわたり長い時間期間にわたって資産を比較するツールを提供し得る。30

【0030】

図示されたモジュール 330 の残りのセットは、構成データベース、監視診断動作視覚化ツール、アナリティクスルールエンジン、ならびにアナリティクスランタイム環境および関連づけられたアプリケーションプログラミングインターフェースおよびサービス指向型アーキテクチャのコレクションである。

【0031】

図 4 を参照すると、本開示の実施形態に係る例示的なオンサイトマネージャ 400 の機能ブロック図が示されている。マネージャ 400 は、1 つ以上のプロセッサ 402、1 つ以上のメモリ 404、1 つ以上の入力／出力（「I/O」）インターフェース 406、および 1 つ以上のネットワークインターフェース 408 を含み得る。マネージャ 400 は、図示されていない他のデバイスを含み得る。40

【0032】

1 つ以上のプロセッサ 402 は、1 つ以上のコアを含み得、1 つ以上のメモリ 404 に記憶された命令に、少なくとも部分的に、アクセスし、同命令を実行するように構成される。1 つ以上のメモリ 404 は、1 つ以上のコンピュータ可読記憶媒体（「CRSM」）を含み得る。1 つ以上のメモリ 404 は、ランダムアクセスメモリ（「RAM」）、フラッシュ RAM、磁気媒体、光学媒体、等を含み得るが、これらに限定されない。1 つ以上

のメモリ 404 は、電力が提供されている間に情報が保持されるという点で揮発性であり得、または、電力の提供なしに情報が保持されるという点で不揮発性であり得る。

【0033】

1つ以上の I/O インターフェース 406 もまた、マネージャ 400 において提供され得る。これらの I/O インターフェース 406 は、センサ、キーボード、マウス、モニタ、プリンタ、外部メモリ、等といったデバイスを結合することを可能にし得る。1つ以上の I/O インターフェース 406 は、システムにわたってオペレーションデータを提供し得るさまざまなセンサおよびコントローラへの結合を可能にし得る。

【0034】

1つ以上のネットワークインターフェース 408 は、ピアツーピアで直接的に、ネットワークを介して、またはその両方で、マネージャ 400 と別のデバイスとの間のデータの転送を提供し得る。1つ以上のネットワークインターフェース 408 は、パーソナルエリアネットワーク（「PAN」）、有線ローカルエリアネットワーク（「LAN」）、広域ネットワーク（「WAN」）、無線ローカルエリアネットワーク（「WLAN」）、無線広域ネットワーク（「WWAN」）、等を含み得るが、これらに限定されない。1つ以上のネットワークインターフェース 408 は、マネージャ 400 と他のデバイスとの間でデータを交換するために、音波、無線周波数、光、または他の信号を利用し得る。

【0035】

1つ以上のメモリ 404 は、ある特定の動作または機能を実行するために1つ以上のプロセッサ 402 によって実行される命令またはモジュールを記憶し得る。以下のモジュールが限定としてではなく例として含まれる。さらに、モジュールはメモリ 404 に記憶されるものとして示されているが、いくつかの実現では、これらのモジュールは、ネットワークインターフェース 408 または I/O インターフェース 406 を介してマネージャ 400 にアクセス可能な外部メモリに少なくとも部分的に記憶され得る。これらのモジュールは、I/O インターフェース 406 のようなハードウェアリソースを管理し、プロセッサ 402 で実行されるアプリケーションまたはモジュールにさまざまなサービスを提供するように構成されたオペレーティングシステムモジュール 410 を含み得る。

【0036】

収集モジュール 414 がメモリ 404 に記憶され得る。モジュール 414 は、1つ以上の入力デバイスからデータを連続的に収集し、さまざまなパラメータを計算するように構成され得る。ソフトウェアモジュール 414 は、ユニットのオペレーションデータと動的なデータ、たとえば、温度、圧力、流量、クリアランス（たとえば、2つのコンポーネント間の距離）、およびターボ機械類の振動データ、の収集に関連づけられ得る。（ネットワーク接続能力 / 生データ分解能に基づいた）さまざまなタイプのコントローラが、ユニットセンサとインターフェース接続するために使用される。コントローラは、M A R K コントローラのようなある特定の専用コントローラから標準的なイーサネット（登録商標）データ収集システム（EDAS）までの範囲にわたり得る。収集された生データが続いて処理され、さまざまなデータハブを介して他の O S M モジュールに転送される。加えて、これらのモジュールは、データ品質および時間の一貫性のために組み合わせられたソースを提供し得る。モジュール 414 は、データベース 412 にデータと計算された推定値とを記憶し得る。

【0037】

処理モジュール 416 は、データを記憶およびアーカイブするように構成され得る。ソフトウェアプラットフォームは、時系列データならびにアノリティクス出力によって生成された処理データのローカルストレージのための能力を提供し得る。それはまた、さまざまな圧縮および内挿技法を使用してデータ品質を管理する能力を提供し得る。

【0038】

転送モジュール 418 は、中央 M & D システムにデータを転送するように構成され得る。一つ目のメカニズムは、リアルタイムデータストリーミングトランスポートを提供するコレクタサービスへのコレクタのために構成され得る。二つ目のメカニズムは、安全（一

10

20

30

40

50

方向トラヒック / プッシュ) で信頼できる非同期並行ファイルトランスポーツトのために低帯域幅のインテリジェントエージェントモジュールによって提供されるサービスを組み合わせ得る。

【 0 0 3 9 】

図 4 に関連して上述されたマネージャ 4 0 0 は、例として提供されているにすぎない。所望のとおり、多数の他の実施形態、システム、方法、装置、およびコンポーネントが、臨界温度を下回るガスタービン焼成温度を制御するために利用され得る。

【 0 0 4 0 】

図 5 は、本開示の実施形態に係るオンサイト監視システムと中央監視診断インフラストラクチャとの間でのデータの例示的な安全なファイルアップロードを示すフローチャート 10 5 0 0 である。

【 0 0 4 1 】

ブロック 5 1 0 において、低帯域幅のエクスポートサービスが、アーカイバモジュールからデータを抽出し得る。ブロック 5 1 0 の後にブロック 5 2 0 が続き、出力ファイルがアップロード / ダウンロードディレクトリに書き込まれ得る。ブロック 5 3 0 において、非同期バックグラウンドインテリジェント転送サービスがスケジューリングされ得る。

【 0 0 4 2 】

ブロック 5 4 0 において、インテリジェントエージェントが、OSM と関連づけられた中央ファイル転送サーバとの間に、安全で（証明書に基づいた）、一方向の（ネットワーキングポート 4 4 3 を使用した）、TLS / SSL 暗号化リンクを確立し得る。 20

【 0 0 4 3 】

ブロック 5 5 0 において、インテリジェントエージェントが、非同期並行並列ファイルアップロードのためのコマンドアップロードメッセージを起動し得る。ブロック 5 6 0 がブロック 5 5 0 の後に続き、インテリジェントエージェントが、関連づけられた HTTP S チャンクを作成し得、ブロック 5 7 0 において、予め選択されたポート（この例ではポート 4 4 3 ）にわたり直列にデータグラムを送信し得る。データトランSPORT の信頼度が、（各チャンクおよび完全なファイルの）チェックサムによって、ならびに、基礎をなすトランSPORT プロトコルスタッカクによって提供される再送メカニズムおよび障害許容メカニズムによって実行される。ブロック 5 8 0 がブロック 5 7 0 の後に続き、HTTP S データグラムが、エージェントサーバサービスによって再構成され、低帯域幅のインポートサービスに提示され得る。 30

【 0 0 4 4 】

図 6 は、本開示の実施形態に係るオンサイト監視システムと中央監視診断インフラストラクチャとの間でのデータの例示的な安全なファイルダウンロードを示すフローチャート 6 0 0 である。

【 0 0 4 5 】

ブロック 6 1 0 において、予め選択されたトラヒックポート（ポート 4 4 3 ）が一方向であり得る（アウトバウンドのみに開いている）ので、エージェントサーバが、インテリジェントエージェントからの任意の以前のメッセージに対する応答内でファイルダウンロード要求メッセージを起動する。ブロック 6 1 0 の後にブロック 6 2 0 が続き、インテリジェントエージェントが、非同期並行並列ファイルダウンロードのためのダウンロードコマンドメッセージを起動し得る。ブロック 6 3 0 において、エージェントサーバが、関連づけられた HTTP S チャンクを作成し、ブロック 6 4 0 において、インテリジェントエージェントにより以前に開かれた接続を使用してポート（ポート 4 4 3 ）にわたり直列にデータグラムを送信する。データトランSPORT の信頼度が、（各チャンクおよび完全なファイルの）チェックサムによって、ならびに、基礎をなすトランSPORT プロトコルスタッカクによって提供される再送メカニズムおよび障害許容メカニズムによって、エージェントサーバにより実行される。最後に、ブロック 6 5 0 において、HTTP S データグラムが、インテリジェントエージェントサーバサービスによって再構成され、低帯域幅のエクスポートサービスに提示される。 40 50

【0046】

図7は、オンサイト監視システムへの例示的な安全なリモートアクセスを示すフローチャート700である。通信セキュリティは、リモートアクセスセッションデータをカプセル化するTLS/SSLベースのトンネリング方法を使用して提供される。

【0047】

ブロック710において、ユーザがオンサイト監視システムへのリモートデスクトッププロトコル(RDP)接続を要求し得る。ブロック720において、トラヒックポート443が一方向である(アウトバウンドのみに開いている)ので、エージェントサーバが、インテリジェントエージェントからの任意の以前のメッセージに対する応答内でRDPセッション要求メッセージを起動し得る。

10

【0048】

ブロック730において、インテリジェントエージェントがオンサイト監視システム上のRDPサーバに接続する。ブロック740がブロック730の後に続き、インテリジェントエージェントがエージェントサーバでTLS/SSLトンネルを開く。ブロック750において、検査された暗号ライブラリを使用してデータが暗号化され、ブロック760において、インテリジェントエージェントが認証処理を完了させる。最後にブロック780において、接続が確立され得る。エンドツーエンドのRDP接続が、オンサイト監視システムのRDPサーバと、インテリジェントエージェントと、エージェントサーバと、エンドユーザのコンピューティングデバイスとの間の中間接続を接続することによって、確立され得る。

20

【0049】

上で説明し、示した動作および処理は、さまざまな実現において所望される任意の適切な順序で遂行または実行され得る。加えて、ある特定の実現では、動作の少なくとも一部が並列に遂行され得る。さらに、ある特定の実現では、説明された動作より少ないまたは多い動作が実行され得る。

【0050】

記載されたこの説明は、ベストモードを含む本開示のある特定の実施形態を開示するために、また、任意のデバイスまたはシステムを製造および使用することと任意の組み込まれた方法を実行することとを含む本開示のある特定の実施形態の実現を任意の当業者に可能にさせるために、例を使用する。本開示のある特定の実施形態の特許可能な範囲は、請求項において定義され、当業者が想到する他の例を含み得る。そのような他の例は、それらが請求項の文字通りの言語と異なる構造要素を有する場合、または、それらが請求項の文字通りの言語と実質的な違いを有しない均等な構造要素を含む場合、請求項の範囲内にあるものと意図される。

30

【符号の説明】**【0051】**

100 例示的なシステムアーキテクチャ

102 Windows(登録商標)ベースのプラットフォーム/インテリジェントエージェント

104 プロキシ

40

106 オンサイトネットワーク

108 企業ファイアウォール

110 オンサイト監視システム

111 コントローラ

113 イーサネットデータ収集システム(EDAS)

114 中央システムインターネット

115 W SSTハブ

116 エンタープライズトンネリングサーバ/エージェントサーバ

117 CIMPPLICITYハブ

118 リモートエンタープライズサーバ

50

1 1 9	E H I S T O R I A Nコレクタ	
1 1 9	ユーザ	
1 3 0	インターネット	
1 3 4	ユーザ	
2 0 0	オンサイト監視(O S M)	
2 1 0	ソフトウェアモジュール	
2 2 0	ストレージソフトウェアモジュール / ソフトウェアプラットフォーム	
2 3 0	データ処理モジュール	
2 3 1	C E N T R A L C O N D I T I O N A S S E S S M E N T P L A T F O R	
M - L O C A L E D I T I O N (C C A P - L E)		10
2 3 3	C D E ルールエンジンプラットフォーム	
2 3 5	動作エンジン	
2 4 0	転送モジュール	
2 4 1	ヒストリアンコレクタ	
2 4 3	インテリジェントエージェントモジュール	
3 0 0	例示的な中央監視診断インフラストラクチャ	
3 1 0	中央システム転送モジュール	
3 1 1	コレクタサービス	
3 1 3	低帯域幅のインポートサービス	
3 2 0	中央ストレージソフトウェアモジュール / ストレージモジュール	20
3 3 0	図示されたモジュール	
4 0 0	例示的なオンサイトマネージャ	
4 0 2	プロセッサ	
4 0 4	メモリ	
4 0 6	I / O インターフェース	
4 0 8	ネットワークインターフェース	
4 1 0	オペレーティングシステムモジュール	
4 1 2	データベース	
4 1 4	収集モジュール	
4 1 6	処理モジュール	30
4 1 8	転送モジュール	
5 1 0	ロック	
5 2 0	ロック	
5 3 0	ロック	
5 4 0	ロック	
5 5 0	ロック	
5 6 0	ロック	
5 7 0	ロック	
5 8 0	ロック	
6 1 0	ロック	40
6 2 0	ロック	
6 3 0	ロック	
6 4 0	ロック	
6 5 0	ロック	
7 1 0	ロック	
7 2 0	ロック	
7 3 0	ロック	
7 4 0	ロック	
7 5 0	ロック	
7 6 0	ロック	50

770 ブロック
780 ブロック

【図1】

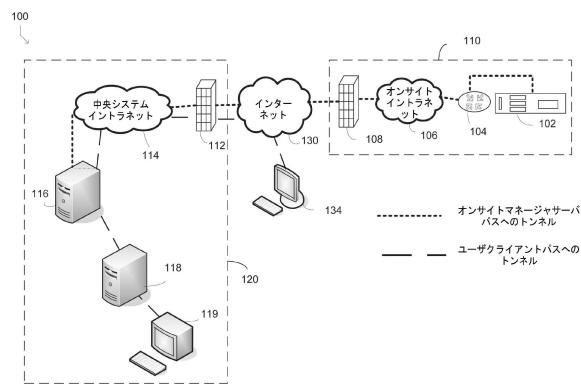


FIG. 1

【図2】

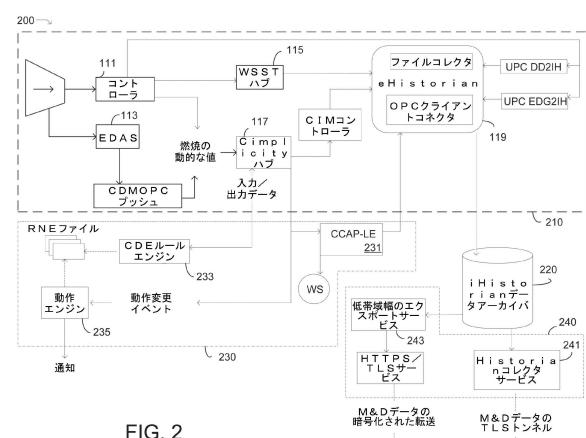


FIG. 2

【図3】

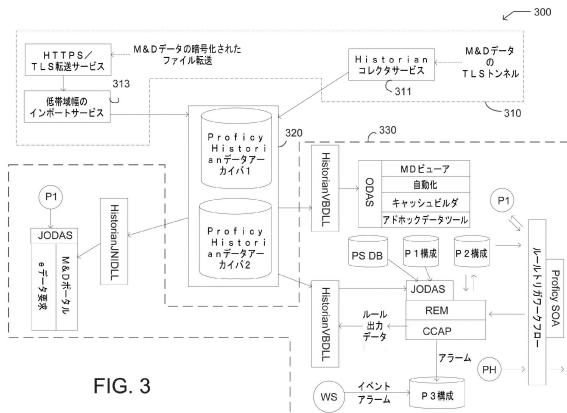


FIG. 3

【図4】

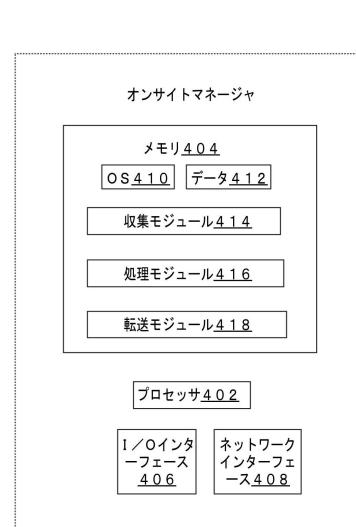


FIG. 4

【図5】

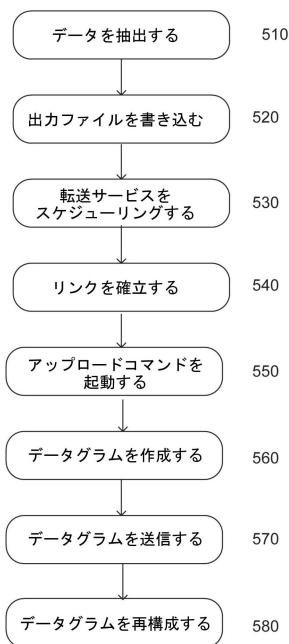


FIG. 5

【図6】

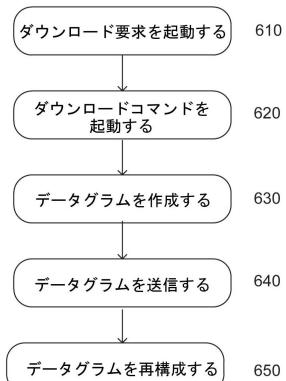


FIG. 6

【図7】

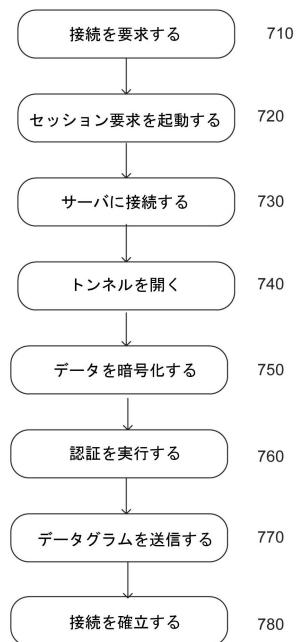


FIG. 7

フロントページの続き

(72)発明者 ユセフ・アタムナ

アメリカ合衆国、ジョージア州、アトランタ、ワイルドウッド・パークウェイ、4200番

審査官 玉木 宏治

(56)参考文献 國際公開第2013/042412 (WO, A1)

特開2000-324157 (JP, A)

特開2001-186912 (JP, A)

高橋 誠, ファイアウォールを越えるリモート監視技術, 計装, (有)工業技術社, 2002年

1月 1日, 第45巻、第1号, pp.61-64

(58)調査した分野(Int.Cl., DB名)

H04L 12/00 - 955