(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6416585号
(P6416585)

(45)発行日　平成30年10月31日(2018.10.31)　(24)登録日　平成30年10月12日(2018.10.12)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	351Z
G06F 21/44	(2013.01)	G06F	21/44	
H04L 9/32	(2006.01)	H04L	9/00	675A
		G06F	13/00	353C

請求項の数 7　外国語出願　(全 16 頁)

(21)出願番号　特願2014-219874 (P2014-219874)
(22)出願日　平成26年10月29日 (2014.10.29)
(65)公開番号　特開2015-92341 (P2015-92341A)
(43)公開日　平成27年5月14日 (2015.5.14)
審査請求日　平成29年10月23日 (2017.10.23)
(31)優先権主張番号　14/072,414
(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・カンパニイ
アメリカ合衆国、ニューヨーク州　１２３４５、スケネクタデイ、リバーロード、１番
(74)代理人　100137545
弁理士　荒川　聡志
(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】安全なリモートアクセス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】
リモートアクセスセッションデータをカプセル化するための方法（７００）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）へのリモート接続の要求をエンドユーザコンピュータ（１１９、１３４）から受信するステップ（７１０）と、
中央システム（１１４）に関連する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）からの以前のメッセージに対する応答内でセッション要求メッセージを起動するステップ（７２０）であって、前記セッション要求メッセージは、アウトバウンド以外の通信を防ぎ、応答以外のメッセージをブロックする予め選択されたトラヒックポートに送られる、起動するステップ（７２０）と、
中央システム（１１４）に関連するオンサイトプロセッサに存在するインテリジェントソフトウェアモジュールにより、前記セッション要求メッセージを受け取るステップと、
前記インテリジェントソフトウェアモジュールにより、前記オンサイトシステム（１１０）とリモート接続サーバ（１１８）との間で接続を確立するステップ（７３０）と、
前記オンサイトシステム（１１０）により前記中央システム（１１４）で安全なトンネルを開くステップ（７４０）と、
前記オンサイトシステム（１１０）により送信のためのデータを暗号化するステップ（７５０）であって、該データは、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からのオペレーショナル情報を含む、暗号化するステップ（７５０）と、

前記オンサイトシステム（１１０）により認証処理を完了させるステップ（７６０）と、
前記エンドユーザコンピュータ（１１９、１３４）と前記オンサイトシステム（１１０）との間で接続を確立するステップ（７８０）と、
前記オンサイトシステム（１１０）から前記エンドユーザコンピュータ（１１９、１３４）に前記データを転送するステップ（７７０）と
を含む、方法（７００）。
【請求項２】
前記オンサイトシステム（１１０）により前記中央システム（１１４）で安全なトンネルを開くこと（７４０）は、セキュアソケットレイヤプロトコルまたはトランスポートレイヤセキュリティを使用するステップを備える、請求項１に記載の方法（７００）。
【請求項３】
前記送信のためのデータを暗号化すること（７５０）は、検査された暗号ライブラリを使用するステップを備える、請求項１に記載の方法（７００）。
【請求項４】
リモートアクセスセッションデータをカプセル化するためのシステム（１００）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）へのリモート接続の要求をエンドユーザコンピュータ（１１９、１３４）から受信するように動作可能な、コンピュータプロセッサを備える中央システム（１１４）を備え、
前記中央システム（１１４）は前記オンサイトシステム（１１０）と通信し、
前記コンピュータプロセッサは、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セッション要求メッセージを起動するように動作可能であり、
前記セッション要求メッセージは、アウトバウンド以外の通信を防ぎ、応答以外のメッセージをブロックする予め選択されたトラヒックポートに送られ、
前記オンサイトシステム（１１０）は、
　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に存在するインテリジェントソフトウェアモジュールにより、前記セッション要求メッセージを受け取り、
　リモートデスクトップサーバ（１１８）に接続し（７３０）、
　前記中央システム（１１４）への安全なトンネルを開き（７４０）、
　前記中央システム（１１４）への送信のためのデータを暗号化し（７５０）、
　認証処理を完了させ（７６０）、
　前記中央システム（１１４）に前記データを送信する（７７０）
ように動作可能であり、
　前記データは、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からのオペレーショナル情報を含む、
システム（１００）。
【請求項５】
前記中央システム（１１４）への安全なトンネルを開くこと（７４０）は、セキュアソケットレイヤプロトコルまたはトランスポートレイヤセキュリティを使用することを備える、請求項４に記載のシステム（１００）。
【請求項６】
前記ファイアウォール（１０８）は、標準的な双方向トランスポート制御プロトコル通信を防止する、請求項４に記載のシステム（１００）。
【請求項７】
前記データは、複数のオンサイトコントローラ（１１１）からのオペレーショナル情報を備える、請求項４に記載のシステム（１００）。

【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、安全なリモートアクセス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、およびサイトへのさまざまな勧告を伴う診断および報告を含み得る。生のオペレーショナルデータだけでなく、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。
【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。
【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る。さらに、すべての標準的な双方向ＴＣＰ／ＨＴＴＰ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。加えて、オンサイト監視に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およびマネジメントタスクを実行する能力を、監視診断ユーザに提供するために、安全なリモートアクセスが必要とされる。
【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】
新たな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、リモートアクセスセッションデータをカプセル化するための方法が開示される。この方法は、インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信することを含み得る。この方法はさらに、中央システムにより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セッション要求メッセージを起動することと、オンサイトシ

ステムとリモート接続サーバとの間で接続を確立することと、オンサイトシステムにより中央システムで安全なトンネルを開くことと、オンサイトシステムにより送信のためのデータを暗号化することと、オンサイトシステムにより認証処理を完了させることと、エンドユーザコンピュータとオンサイトシステムとの間で接続を確立することと、中央システムからオンサイトシステムにデータを転送することとを含み得る。

【０００８】

別の実施形態では、リモートアクセスセッションデータをカプセル化するためのシステムが開示される。このシステムは、インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信するように動作可能な中央システムを含み得る。中央システムは、オンサイトシステムと通信し、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セッション要求メッセージを起動するように動作可能であり得る。オンサイトシステムは、リモートデスクトップサーバに接続し、中央システムへの安全なトンネルを開き、中央システムへの送信のためのデータを暗号化し、認証処理を完了させ、中央システムにデータを送信するように動作可能であり得る。

【０００９】

さらなる別の実施形態では、１つ以上のプロセッサによって実行された場合、インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信し、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セッション要求メッセージを起動し、オンサイトシステムとリモート接続サーバとの間で接続を確立し、オンサイトシステムにより中央システムで安全なトンネルを開き、送信のためのデータを暗号化し、オンサイトシステムにより認証処理を完了させ、エンドユーザコンピュータとオンサイトシステムとの間で接続を確立し、中央システムからオンサイトシステムにデータを転送し得る命令を備える非一時的なコンピュータ可読媒体が開示される。

【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、および態様が、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】図１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】図２は、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】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の模式的なブロック図である。

【図４】図４は、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】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である。

【図６】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である。

【図７】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、添付図面を参照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されることができ、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求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。
【００１４】
発電所のオンサイト監視をサポートする安全なリモート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。本開示の他の実施形態は、オンサイト監視システムへの安全なリモートアクセスを可能にし、ある特定のアドミニストレーションおよびマネジメントタスクの実行を可能にする技術的効果を有し得る。
【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】
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／ＨＴＴＰ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。
【００１８】
中央システムイントラネット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が続いて、オンサイト監視システム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。

【００２０】

図示されたシステム１００は、オンサイトマネジメントシステムへのリモートアクセスサービスの確立を可能にする安全なリモートアクセスソリューションを提供する。この、非同期かつＴＬＳトンネリングベースのＲＤＰソリューションは、通信ポートが典型的にアウトバウンドのみに開いているので、意図的に一方向である。

【００２１】

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）システム２００の例が示されている。ＯＳＭシステム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。

【００２２】

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ナルかつ動的なデータ、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他に監視の自動化を実行し得る。そのようなデータハブは、ＷＳＳＴ１１５、ＣＩＭＰＬＩＣＩＴＹ１１７、およびＥＨＩＳＴＯＲＩＡＮ１１９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。

【００２３】

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 ＨＩＳＴＯＲＩＡＮのような専用プラットフォームであり得、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。

【００２４】

データ処理モジュール２３０は、データ処理だけでなく、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が送られ得る。

【００２５】

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スポートメカニズムが一般的に利用可能である。１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ために、

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。２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行ファイルトランスポートのために、低帯域幅でインテリジェントな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。

【００２６】

したがって、少なくとも１つの技術的効果は、低帯域幅でインテリジェントな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行ファイルトランスポートの提供を可能にさせることができる。

【００２７】

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。

【００２８】

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スポートメカニズムが一般的に利用可能である。１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。２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行ファイルトランスポートのために、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。

【００２９】

中央ストレージソフトウェアモジュール３２０は、データの記憶および最初に収集され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能力を提供し得る。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能力を提供し得る。

【００３０】

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。

【００３１】

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。

【００３２】

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。

【００３３】

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。

【００３４】

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ナル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。

【００３５】

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な、ネットワークを介しての、またはその両方による、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。

【００３６】

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。

【００３７】

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ナルかつ動的なデータ、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、ＭＡＲＫ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ＯＳＭ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。

【００３８】

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。

【００３９】

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。１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。２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行ファイルトランスポー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。

【００４０】

図４に関連して上述されたマネージャ４００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。

【００４１】

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５００である。

【００４２】

ブロック５１０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５１０の後にブロック５２０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５３０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。

【００４３】

ブロック５４０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４４３を使用した）、ＴＬＳ／ＳＳＬ暗号化リンクを確立し得る。

【００４４】

ブロック５５０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５６０がブロック５５０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ＨＴＴＰＳチャンクを作成し得、ブロック５７０において、予め選択されたポート（この例ではポート４４３）にわたり直列にデータグラムを送り得る。データトランスポートの信頼度が、（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、基礎をなすトランスポートプロトコルスタッ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５８０がブロック５７０の後に続き、ＨＴＴＰＳ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。

【００４５】

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６００である。

【００４６】

ブロック６１０において、予め選択されたトラヒックポート（ポート４４３）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６１０の後にブロック６２０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６３０において、エージェントサーバが、関連づけられたＨＴＴＰＳチャンクを作成し、ブロック６４０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４４３）にわたり直列にデータグラムを送る。データトランスポートの信頼度が、（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、基礎をなすトランスポートプロトコルスタッ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６５０において、ＨＴＴＰＳ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。

【００４７】
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。
【００４８】
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。
【００４９】
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。
【００５０】
上に説明し、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。
【００５１】
記載されたこの説明は、最良の形態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らない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。
［実施態様１］
リモートアクセスセッションデータをカプセル化するための方法であって、
インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信することと、
中央システムにより前記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セッション要求メッセージを起動することと、
前記オンサイトシステムとリモート接続サーバとの間で接続を確立することと、
前記オンサイトシステムにより前記中央システムで安全なトンネルを開くことと、
前記オンサイトシステムにより送信のためのデータを暗号化することと、
前記オンサイトシステムにより認証処理を完了させることと、
前記エンドユーザコンピュータと前記オンサイトシステムとの間で接続を確立することと、
前記中央システムから前記オンサイトシステムに前記データを転送することと
を備える方法。
［実施態様２］
前記オンサイトシステムにより前記中央システムで安全なトンネルを開くことは、セキ

ュアソケットレイヤプロトコルまたはトランスポートレイヤセキュリティを使用することを備える、実施態様１に記載の方法。
［実施態様３］
前記送信のためのデータを暗号化することは、検査された暗号ライブラリを使用することを備える、実施態様１に記載の方法。
［実施態様４］
前記ファイアウォールは、標準的な双方向トランスポート制御プロトコル通信を防止する、実施態様１に記載の方法。
［実施態様５］
前記セッション要求メッセージを起動することは、開いているアウトバウンド一方向ポートに前記メッセージを送ることを備える、実施態様１に記載の方法。
［実施態様６］
前記エンドユーザコンピュータは、中央システムファイアウォールの背後にある、実施態様１に記載の方法。
［実施態様７］
前記エンドユーザコンピュータは、中央システムファイアウォールの中にない、実施態様１に記載の方法。
［実施態様８］
前記データは、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からのオペレーショナル情報を備える、実施態様１に記載の方法。
［実施態様９］
前記データのアナリティクスおよび／または診断を実行することをさらに備える、実施態様１に記載の方法。
［実施態様１０］
リモートアクセスセッションデータをカプセル化するためのシステムであって、
インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信するように動作可能な中央システムを備え、
前記中央システムは、前記オンサイトシステムと通信し、前記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セッション要求メッセージを起動するように動作可能であり、
前記オンサイトシステムは、
リモートデスクトップサーバに接続し、
前記中央システムへの安全なトンネルを開き、
前記中央システムへの送信のためのデータを暗号化し、
認証処理を完了させ、
前記中央システムに前記データを送信する
ように動作可能である、システム。
［実施態様１１］
前記中央システムへの安全なトンネルを開くことは、セキュアソケットレイヤプロトコルまたはトランスポートレイヤセキュリティを使用することを備える、実施態様１０に記載のシステム。
［実施態様１２］
前記ファイアウォールは、標準的な双方向トランスポート制御プロトコル通信を防止する、実施態様１０に記載のシステム。
［実施態様１３］
前記中央システムが前記セッション要求メッセージを起動する際、前記中央システムはさらに、開いているアウトバウンド一方向ポートに前記メッセージを送るように動作可能である、実施態様１０に記載のシステム。
［実施態様１４］

前記リモートデスクトップサーバと、前記エンドユーザコンピュータと、前記中央システムと、前記オンサイトシステムとの間で、リモート接続が確立される、実施態様１０に記載のシステム。

［実施態様１５］

前記エンドユーザコンピュータは、中央システムファイアウォールの背後にある、実施態様１０に記載のシステム。

［実施態様１６］

前記エンドユーザコンピュータは、中央システムファイアウォールの背後にない、実施態様１０に記載のシステム。

［実施態様１７］

前記データは、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からのオペレーショナル情報を備える、実施態様１０に記載のシステム。

［実施態様１８］

前記データは、複数のオンサイトコントローラからのオペレーショナル情報を備える、実施態様１０に記載のシステム。

［実施態様１９］

命令を備える１つ以上の非一時的なコンピュータ可読媒体であって、前記命令は、１つ以上のプロセッサによって実行された場合、

インバウンド接続を防止するファイアウォールの背後のオンサイトシステムへのリモート接続の要求をエンドユーザコンピュータから受信し、

中央システムにより前記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セッション要求メッセージを起動し、

前記オンサイトシステムとリモート接続サーバとの間で接続を確立し、

前記オンサイトシステムにより前記中央システムで安全なトンネルを開き、

送信のためのデータを暗号化し、

前記オンサイトシステムにより認証処理を完了させ、

前記エンドユーザコンピュータと前記オンサイトシステムとの間で接続を確立し、

前記中央システムから前記オンサイトシステムに前記データを転送する

動作を実行する、１つ以上の非一時的なコンピュータ可読媒体。

【符号の説明】

【００５２】

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
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　中央システムイントラネット
１１５　ＷＳＳＴ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　ＣＩＭＰＬＩＣＩＴＹハブ
１１８　リモートエンタープライズサーバ
１１９　ＥＨＩＳＴＯＲＩＡＮコレクタ
１１９　ユーザ
１３０　インターネット
１３４　ユーザ
２００　オンサイト監視（ＯＳＭ）システム

２１０　ソフトウェアモジュール
２２０　ストレージソフトウェアモジュール
２３０　データ処理モジュール
２３１　ＣＥＮＴＲＡＬ　ＣＯＮＤＩＴＩＯＮ　ＡＳＳＥＳＳＭＥＮＴ　ＰＬＡＴＦＯＲＭ－ＬＯＣＡＬ　ＥＤＩＴＩＯＮ（ＣＣＡＰ－ＬＥ）
２３３　ＣＤＥルールエンジンプラットフォーム
２３５　動作エンジン
２４０　転送モジュール
２４１　ヒストリアンコレクタ
２４３　インテリジェントエージェントモジュール
３００　例示的な中央監視診断インフラストラクチャ
３１０　中央システム転送モジュール
３１１　コレクタサービス
３１３　低帯域幅のインポートサービス
３２０　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
３３０　図示されたモジュール
４００　例示的なオンサイトマネージャ
４０２　プロセッサ
４０４　メモリ
４０６　Ｉ／Ｏインターフェース
４０８　ネットワークインターフェース
４１０　オペレーティングシステムモジュール
４１２　データベース
４１４　収集モジュール
４１６　処理モジュール
４１８　転送モジュール
５００　フローチャート
５１０　ブロック
５２０　ブロック
５３０　ブロック
５４０　ブロック
５５０　ブロック
５６０　ブロック
５７０　ブロック
５８０　ブロック
６００　フローチャート
６１０　ブロック
６２０　ブロック
６３０　ブロック
６４０　ブロック
６５０　ブロック
７００　フローチャート
７１０　ブロック
７２０　ブロック
７３０　ブロック
７４０　ブロック
７５０　ブロック
７６０　ブロック
７７０　ブロック
７８０　ブロック

【図１】

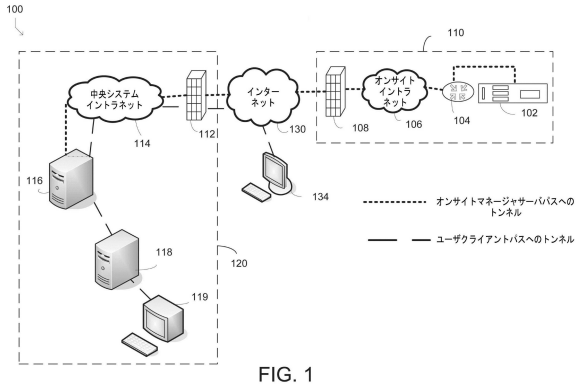

FIG. 1

【図２】

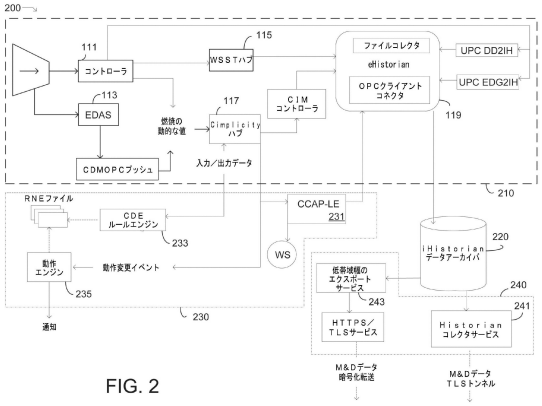

FIG. 2

【図３】

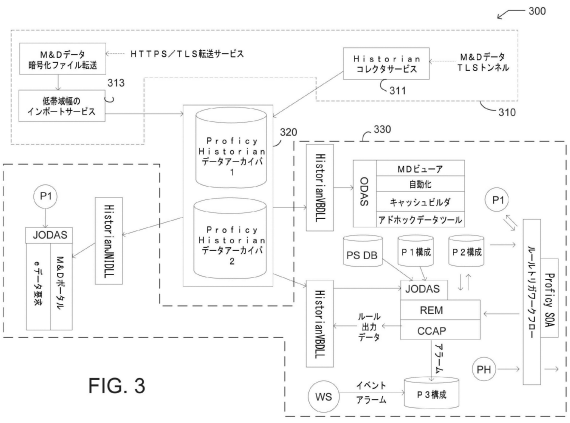

FIG. 3

【図４】

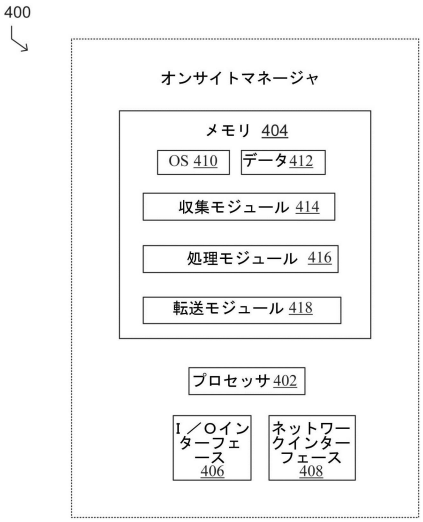

FIG. 4

【図５】

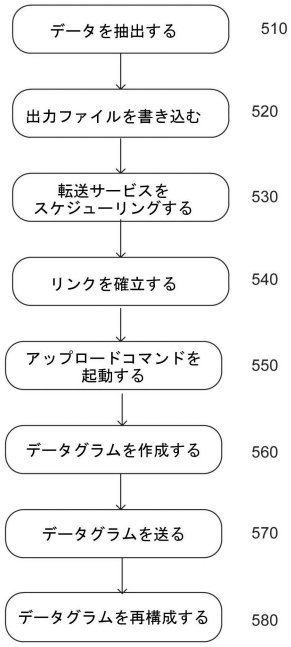

FIG. 5

【図６】

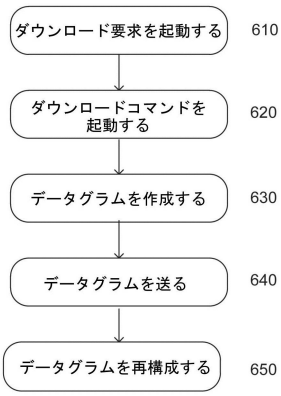

FIG. 6

【図７】

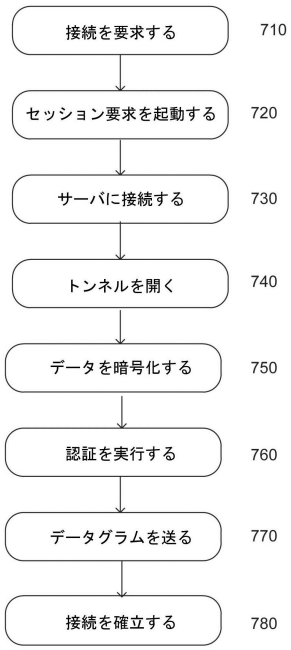

FIG. 7

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　安藤　一道

(56)参考文献　米国特許第０７５６５５２６（ＵＳ，Ｂ１）
中国実用新案第２０１１８８６２６（ＣＮ，Ｙ）
国際公開第２００７／０４４８３２（ＷＯ，Ａ２）
国際公開第２０１３／０１２６５４（ＷＯ，Ａ２）
米国特許出願公開第２０１３／０３１７６５９（ＵＳ，Ａ１）
米国特許出願公開第２００９／０２２２８８５（ＵＳ，Ａ１）
米国特許出願公開第２００８／０１０９８８９（ＵＳ，Ａ１）
米国特許出願公開第２００３／０１２６４６８（ＵＳ，Ａ１）
米国特許第０８５９５８３１（ＵＳ，Ｂ２）
特表２０１４－５２６０９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　２１／４４
Ｈ０４Ｌ　９／３２