(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5965478号
(P5965478)
(45)発行日　平成28年8月3日(2016.8.3)　(24)登録日　平成28年7月8日(2016.7.8)

(51)Int.Cl.　　F I
G06F 21/44 (2013.01)　　G06F 21/44
G09C 1/00 (2006.01)　　G09C 1/00　640D

請求項の数 20　(全 12 頁)

(21)出願番号　特願2014-513794(P2014-513794)
(86)(22)出願日　平成24年6月4日(2012.6.4)
(65)公表番号　特表2014-517406(P2014-517406A)
(43)公表日　平成26年7月17日(2014.7.17)
(86)国際出願番号　PCT/US2012/040775
(87)国際公開番号　WO2012/167268
(87)国際公開日　平成24年12月6日(2012.12.6)
審査請求日　平成27年5月18日(2015.5.18)
(31)優先権主張番号　61/493,330
(32)優先日　平成23年6月3日(2011.6.3)
(33)優先権主張国　米国(US)

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
特許業務法人深見特許事務所
(72)発明者　ヨンセン，ビョルン－ダグ
ノルウェー、エヌ－０６８７　オスロ、ビルベルクグレンダ、９
(72)発明者　ホドバ，プレドラグ
ノルウェー、エヌ－１３８９　ヘッゲダール、ホイマイルフェレット、１０

最終頁に続く

(54)【発明の名称】ネットワークにおけるコンポーネントを認証するためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
InfiniBand（ＩＢ）ファブリックにおけるファブリックコンポーネントの信頼性を検証する方法であって、
ＩＢファブリックにおけるファブリックコンポーネントに第１の暗号化されたメッセージをサブネットマネージャを介して送信するステップを備え、前記第１の暗号化されたメッセージはトークンを含み、前記ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化され、方法はさらに、
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた秘密キーを使用して前記第１の暗号化されたメッセージを復号化させ、前記サブネットマネージャへ第２の暗号化されたメッセージを送信させるステップと、
前記第２の暗号化されたメッセージが正しい情報を含む場合にサブネットマネージャを介して前記ファブリックコンポーネントを認証するステップとを備える、方法。
【請求項２】
前記ファブリックコンポーネントをテナントに指定されたホストチャンネルアダプタ（ＨＣＡ）ファームウェアまたはハイパーバイザ／ＯＳとするステップをさらに備える、請求項１に記載の方法。
【請求項３】
前記第１の暗号化されたメッセージに含まれる前記トークンをランダムバイトストリングとするステップをさらに備える、請求項１または２に記載の方法。

【請求項４】
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた前記秘密キーを埋込型ファームウェアに隠させるステップをさらに備える、請求項１から３のいずれかに記載の方法。
【請求項５】
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた前記秘密キーをタンパー防止不揮発性キー記憶部に記憶させるステップをさらに備える、請求項１から４のいずれかに記載の方法。
【請求項６】
前記ファブリックコンポーネントと関連付けられた前記公開キーをレポジトリに記憶するステップをさらに備える、請求項１から５のいずれかに記載の方法。
【請求項７】
前記サブネットマネージャと関連付けられた公開キーを前記第１の暗号化されたメッセージと併せて前記ファブリックコンポーネントに対して送信するステップをさらに備える、請求項１から６のいずれかに記載の方法。
【請求項８】
前記ファブリックコンポーネントに前記サブネットマネージャと関連付けられた前記公開キーを使用して前記第２の暗号化されたメッセージを暗号化させるステップをさらに備える、請求項７に記載の方法。
【請求項９】
前記サブネットマネージャと関連付けられた秘密キーを使用して前記第２の暗号化されたメッセージを当該サブネットマネージャを介して復号化するステップをさらに備える、請求項８に記載の方法。
【請求項１０】
前記第２の暗号化されたメッセージに関して前記サブネットマネージャに対して前記トークンが返信された場合にのみ前記ファブリックコンポーネントを認証するステップをさらに備える、請求項１から９のいずれかに記載の方法。
【請求項１１】
InfiniBand（ＩＢ）ファブリックにおけるファブリックコンポーネントの信頼性を検証するためのシステムであって、
前記ＩＢファブリックにおけるファブリックコンポーネントを認証する役割を担うサブネットマネージャを備え、
前記サブネットマネージャは、
前記ＩＢファブリックにおける前記ファブリックコンポーネントに第１の暗号化されたメッセージを送信するように構成され、前記第１の暗号化されたメッセージはトークンを含み、前記ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化され、前記サブネットマネージャはさらに、
前記ファブリックコンポーネントに当該ファブリックコンポーネントと関連付けられた秘密キーを使用して前記第１の暗号化されたメッセージを復号化させ、前記サブネットマネージャへ第２の暗号化されたメッセージを送信させ、
前記第２の暗号化されたメッセージが正しい情報を含む場合に前記ファブリックコンポーネントを認証するように構成される、システム。
【請求項１２】
前記ファブリックコンポーネントは、テナントに指定されたホストチャンネルアダプタ（ＨＣＡ）ファームウェアまたはハイパーバイザ／ＯＳである、請求項１１に記載のシステム。
【請求項１３】
前記第１の暗号化されたメッセージに含まれる前記トークンは、ランダムバイトストリングである、請求項１１または１２に記載のシステム。
【請求項１４】

前記ファブリックコンポーネントは、当該ファブリックコンポーネントと関連付けられた前記秘密キーを埋込型ファームウェアに隠す、請求項１１から１３のいずれかに記載のシステム。

【請求項１５】

前記ファブリックコンポーネントは、当該ファブリックコンポーネントと関連付けられた前記秘密キーをタンパー防止不揮発性キー記憶部に記憶する、請求項１１から１４のいずれかに記載のシステム。

【請求項１６】

前記ファブリックコンポーネントと関連付けられた前記公開キーをレポジトリに記憶する、請求項１１から１５のいずれかに記載のシステム。

【請求項１７】

前記サブネットマネージャと関連付けられた公開キーが前記暗号化されたメッセージと併せて前記ファブリックコンポーネントに対して送信される、請求項１１から１６のいずれかに記載のシステム。

【請求項１８】

前記ファブリックコンポーネントは、前記サブネットマネージャと関連付けられた前記公開キーを使用して前記第２の暗号化されたメッセージを暗号化するように動作する、請求項１７に記載のシステム。

【請求項１９】

前記サブネットマネージャは、

前記サブネットマネージャと関連付けられた秘密キーを使用して前記第２の暗号化されたメッセージを復号化し、

前記第２の暗号化されたメッセージにおいて前記サブネットマネージャに前記トークンが返信された場合にのみ前記ファブリックコンポーネントを認証するように動作する、請求項１８に記載のシステム。

【請求項２０】

請求項１から１０のいずれかに記載の方法をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

著作権についての注意

この特許文献の開示の一部には、著作権の保護対象となる資料が含まれている。著作権者は、特許商標庁の特許ファイルまたは記録に記載されたとおりのものについては、特許文献または特許の開示を他人が複製することに異議を唱えないが、他の点については、全ての著作権を確保している。

【０００２】

発明の分野

本発明は、概してコンピュータシステムに関し、特定的にはInfiniBand（ＩＢ）ネットワークを支持することに関する。

【背景技術】

【０００３】

背景

相互接続ネットワークは、スーパーコンピュータ、クラスタ、およびデータセンタの次世代において有益な役割を担っている。InfiniBand（ＩＢ）技術などの高性能ネットワーク技術は、高帯域および低レイテンシが重要な要件となる高性能ドメインにおいて、専用もしくは低性能ソリューションに取って代わるものとなっている。たとえば、ＩＢのインストールは、ロスアラモス国立研究所（Los Alamos National Laboratory）のRoadrunner、テキサス先端算出センター（Texas Advanced Computing Center）のRanger、およびユーリヒ総合研究機構（Forschungszcntrum Juelich）のJuRoPaなどのスーパーコンピュー

タにおいて使用される。

【０００４】

ＩＢは、Future I/OおよびNext Generation I/Oと呼ばれる２つの旧来技術を融合したものとして２０００年１０月にまず標準化された。その低レイテンシ、高帯域、およびホスト側処理リソースの有効利用により、大きくスケーラブルなコンピュータクラスタを構築するためのソリューションとして高性能コンピューティング（ＨＰＣ）コミュニティ内で受け入れられている。事実上のＩＢ用システムソフトウェアは、専門家によって開発されてオープン・ファブリックス・アライアンス（OpenFabrics Alliance）によって保全されているオープン・ファブリックス・エンタープライズ・ディストリビューション（Open Fabrics Enterprise Distribution）（ＯＦＥＤ）である。ＯＦＥＤは、オープンソースであり、GNU/Linux（登録商標）およびMicrosoft Windows（登録商標）の両方において使用可能である。

【発明の概要】

【課題を解決するための手段】

【０００５】

概要

InfiniBand（ＩＢ）ファブリックにおけるファブリックコンポーネントの信頼性を検証することができるシステムおよび方法がここに記載される。サブネットマネージャは、秘密キー／公開キーのペアを使用してファブリックコンポーネントを認証する役割を担う。サブネットマネージャは、ＩＢファブリックにおけるファブリックコンポーネントに第１の暗号化されたメッセージをまず送ることができる。第１の暗号化されたメッセージはトークンを含み、ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化される。そして、ファブリックコンポーネントは、ファブリックコンポーネントと関連付けられた公開キーを使用して第１の暗号化されたメッセージを復号化し、第２の暗号化されたメッセージをサブネットマネージャに返信することができる。最後に、サブネットマネージャは、第２の暗号化されたメッセージが正しい情報を含む場合にファブリックコンポーネントを認証することができる。

【図面の簡単な説明】

【０００６】

【図１】発明の実施形態に基づくミドルウェア環境におけるファブリックモデルを示す図である。

【図２】発明の実施形態に基づくＩＢファブリックにおいて発見されたコンポーネントを認証するための公開／秘密キーに基づいたスキームの使用を示す図である。

【図３】発明の実施形態に基づくＩＢファブリックにおいて発見されたコンポーネントを認証するための公開／秘密キーに基づいたスキームの使用についての例示的なフローチャートを示す図である。

【発明を実施するための形態】

【０００７】

詳細な説明

InfiniBand（ＩＢ）ネットワークなどの相互接続ネットワークにおける様々なコンポーネントの信頼性の検証を支持するシステムおよび方法がここに記載される。

【０００８】

図１は、発明の実施形態に基づくミドルウェア環境におけるファブリックモデルを示す図である。図１に示されるように、相互接続ネットワークまたはファブリック１００は、スイッチ１０１～１０３と、ブリッジおよびルータ１０４と、ホストチャンネルアダプタ（ＨＣＡ）１０５～１０６と、指定された管理ホスト１０７とを含み得る。加えて、ファブリックは、指定された管理ホストではない１つ以上のホスト１０８を含み得る、またはこのホスト１０８に接続され得る。

【０００９】

指定された管理ホスト１０７には、ネットワーク管理タスクを実行するために、ＨＣＡ

１０５～１０６、ネットワークソフトウェアスタック、および関連する管理ソフトウェアがインストールされ得る。さらに、ファブリックにおけるトラフィックの流れを方向付けするために、スイッチ１０１～１０３ならびにブリッジおよびルータ１０４にファームウェアおよび管理ソフトウェアが配置され得る。ここで、指定された管理ホストではないホスト１０８上のホストＨＣＡドライバ、ＯＳ、およびハイパーバイザは、管理の観点から、ファブリックの範囲外にあると考えてもよい。

【００１０】

ファブリック１００は、たとえばＩＢのみのファブリックなど、単一のメディアタイプとし、完全に接続することができる。ファブリックにおける物理的な接続性により、劣化のない場合において、すべてのファブリックコンポーネント間の帯域内接続性が確実なものとなる。代替的に、ファブリックは、ゲートウェイ１０９のゲートウェイ（ＧＷ）外部ポート外のイーサネット（登録商標）（Enet）接続性を含むように構成することができる。加えて、より大きなシステムの一部として並行して動作する独立したファブリックを有することもできる。たとえば、異なるファブリックは、異なるＨＣＡもしくはＨＣＡポートを介して間接的にのみ接続することができる。

【００１１】

InfiniBand（ＩＢ）アーキテクチャ

ＩＢアーキテクチャは、直列ポイントツーポイント技術である。ＩＢネットワークもしくはサブネットの各々は、スイッチおよびポイントツーポイントリンクを使用して相互に接続されるホストのセットを含むことができる。単一のサブネットは、一万を超えるノードに拡張することができ、ＩＢルータを使用して２つ以上のサブネットを相互接続させることができる。サブネット内のホストおよびスイッチは、ローカル識別子（ＬＩＤ）を使用してアドレスが指定される。たとえば、単一のサブネットは、４９１５１個のユニキャストアドレスに限定され得る。

【００１２】

ＩＢサブネットは、サブネットにおけるスイッチ、ルータ、およびホストチャンネルアダプタ（ＨＣＡ）にある全てのＩＢポートの構成を含むサブネットを初期化して始動させる役割を担う少なくとも１つのサブネットマネージャ（ＳＭ）を用いることができる。ＳＭの役割には、ルーティングテーブルの算出および配置も含まれる。ネットワークのルーティングは、全てのソースおよび接続先のペア間において完全な接続性、無デッドロック性、および負荷の均衡を得ることを目的としている。ルーティングテーブルは、ネットワークの初期化時において算出することができ、この処理は、ルーティングテーブルを更新して最適な性能を確実なものとするために、トポロジが変化する時に繰り返し行うことができる。

【００１３】

初期化時において、全てのスイッチおよびホストを発見するためにＳＭがネットワークをスイープする発見段階にＳＭが始動する。発見段階の間、ＳＭは、存在するすべての他のＳＭを発見し、どれをマスターＳＭとするべきかについての交渉を行う。発見段階が完了すると、ＳＭはマスター段階に入ることができる。マスター段階において、ＳＭはＬＩＤの指定、スイッチの構成、ルーティングテーブルの算出および配置、ならびにポートの構成を進める。この時点でサブネットは起動され、使用の準備が整う。

【００１４】

サブネットが構成された後、ＳＭはネットワークの変化（たとえば、リンクが切れる、装置が追加される、またはリンクが除去される）をモニタリングすることができる。モニタリング処理中に変化が検知されると、メッセージ（たとえば、トラップ）をＳＭに転送することができ、ＳＭはネットワークを再構成することができる。再構成処理の一部、または重度のスイープ処理は、完全な接続性および無デッドロック性を保証し、全てのソースおよび接続先のペア間における負荷の適切な均衡化を確実なものとするために行うことのできるネットワークのルートの再指定である。

【００１５】

ＩＢネットワークにおけるＨＣＡは、キューペア（ＱＰ）を使用して互いに通信することができる。ＱＰは、通信設定時に作成され、ＱＰ番号、ＨＣＡポート、接続先ＬＩＤ、キューサイズ、および伝達サービスなどの初期属性のセットが与えられる。他方、通信においてＨＣＡと関連付けられたＱＰは、通信が終了した時に破棄される。ＨＣＡは、多くのＱＰを扱うことができる。各ＱＰは、送信キュー（ＳＱ）と受信キュー（ＲＱ）とのキューのペアからなる。通信に参加する各エンドノードに１つのこのようなペアが存在する。送信キューは、遠隔ノードに伝送される作業要求を保持し、受信キューは、遠隔ノードから受信したデータで何をするかについての情報を保持する。ＱＰに加え、各ＨＣＡは、送信キューと受信キューとのセットに関連付けられた１つ以上の完了キュー（ＣＱ）を有することができる。ＣＱは、送信キューおよび受信キューに提示された作業要求についての完了通知を保持する。

【００１６】

ＩＢアーキテクチャは柔軟なアーキテクチャである。ＩＢサブネットの構成および保全は、特殊な帯域内サブネット管理パケット（ＳＭＰ）を介して行うことができる。ＳＭの機能は、原則として、ＩＢサブネット内のすべてのノードから実施することができる。ＩＢサブネットにおける各エンドポートは、対象となるＳＭＰベースの要求パケットを扱う役割を担う関連付けられたサブネット管理エージェント（ＳＭＡ）を有することができる。ＩＢアーキテクチャにおいて、同じポートは、ＳＭインスタンス、またはＳＭＰベースの通信を使用する他のソフトウェアコンポーネントを示すことができる。したがって、明確に定義されたＳＭＰ動作のサブセットのみがＳＭＡによって扱われ得る。

【００１７】

ＳＭＰは、たとえばフロー制御されていない特殊な仮想レーン（ＶＬ１５）など、ファブリックにおける専用のパケットバッファリソースを使用する（すなわち、ＳＭＰパケットは、バッファがオーバーフローした場合にドロップされてもよい）。また、ＳＭＰは、エンドポートローカル識別子（ＬＩＤ）に基づいてＳＭが設定するルーティングを使用することができる、または、ＳＭＰは、ルートが送信者によって完全に定義されてパケットに埋め込まれた直接ルートを使用することができる。直接ルートを使用し、パケットの経路はＨＣＡおよびスイッチのポート番号の順にファブリックを通過する。

【００１８】

ＳＭは、各スイッチおよび／または各ＨＣＡにおいて示されるＳＭＡを使用してネットワークの変化をモニタ監視することができる。ＳＭＡは、新しい接続、切断、ポートの状態変化などの変化をトラップおよび通知を使用してＳＭに通信する。トラップは、特定のイベントについてエンドノードに警告するために送信されるメッセージである。トラップは、イベントの詳細を記載した通知の属性を含むことができる。異なるイベントについて異なるトラップを定義することができる。トラップの不要な配信を減らすために、ＩＢはイベント転送機構を適用する。このイベント転送機構において、エンドノードは、知らせてほしいトラップについて規則的に受け取ることを明示的に要求する必要がある。

【００１９】

サブネットアドミニストレータ（ＳＡ）は、サブネットについての異なる情報を格納するためにマスターＳＭに関連付けられたサブネットデータベースである。ＳＡとの通信は、ＱＰ１などの指定されたＱＰを介してジェネラルサービスマネージメントデータグラム（ＭＡＤ）を送信することにより、エンドノードによるＱＰの確立を補助することができる。送信側および受信側の両方が、ＱＰを介した通信を確立するために、ソース／接続先ＬＩＤ、サービスレベル（ＳＬ）、最大転送単位（ＭＴＵ）などの情報を必要とする。この情報は、ＳＡによって提供される経路記録として知られるデータ構造から検索することができる。経路記録を取得するために、エンドノードは、たとえばSubnAdmGet／SubnAdmGetable操作を使用して、経路記録クエリをＳＡに対して送信することができる。そして、ＳＡは要求された経路記録をエンドノードに対して返信することができる。

【００２０】

ＩＢアーキテクチャは、どのＩＢエンドポートが他のどのＩＢエンドポートと通信でき

るようにすべきかを定義する方法として、パーティションを提供する。パーティションは、ＩＢファブリック上の全ての非ＳＭＰパケットについて定義される。デフォルトパーティション以外のパーティションは、任意で使用される。パケットのパーティションは、１５ビットのパーティション番号と単一ビットのメンバータイプ（フルまたは限定）からなる１６ビットのP_Keyによって定義することができる。

【００２１】

ホストポートまたはＨＣＡポートのパーティションのメンバーシップは、ホストの現在のパーティションメンバーシップ指針に対応するP_Key値を用いてポートのP_Keyテーブルをｓｍが設定するという前提に基づき得る。ホストが完全に信用されない可能性を補償するために、ＩＢアーキテクチャは、パーティションを実行するために任意でスイッチポートを設定することができることを定義する。これ故に、ホストポートに接続するスイッチポートのP_Keyテーブルは、ホストポートがメンバーであるはずの同じパーティションを反映するように設定することができる（すなわち、イーサネット（登録商標）ＬＡＮにおいて実行されるＶＬＡＮ制御の切り替えと本質的に同等である）。

【００２２】

ＩＢアーキテクチャはＳＭＰを介したＩＢサブネットの完全な帯域内の構成および保守を可能とすることから、ＳＭＰ自体はパーティションメンバーシップによる制限の対象とはならない。したがって、ＩＢファブリック上において不明確なノードもしくは危殆化されたノードが任意のファブリック構成（パーティションメンバーシップを含む）を定義できないように、他の保護機構が必要となる。

【００２３】

ＳＭＰへのアクセスのためのＩＢアーキテクチャにおける基本的な保護／保安機構としてM_Keyを使用することができる。M_Keyは、ＩＢサブネットにおける各個別のノードと個別に関連付けることができる６４ビットの値であり、ＳＭＰが正しいM_Key値を含むかどうかに応じて、入力されるＳＭＰ操作がターゲットノードによって容認もしくは拒絶され得る（すなわち、P_Keysとは異なり、パスワードのような、正しいM_Key値を特定する能力がアクセス制御を示す）。

【００２４】

スイッチと関連付けられたM_Keyを定義するための帯域外の方法を使用することにより、ローカルスイッチポートについてのパーティションメンバーシップを含むスイッチ構成をホストノードが設定できないようにすることを確実とすることができる。したがって、M_Key値は、スイッチＩＢリンクが稼働したときに定義される。これ故に、M_Key値が危殆化されていないもの、もしくは「推測」されないものであり、スイッチ帯域外アクセスが安全であり、認証されたファブリックアドミニストレータのみに限定されている限り、ファブリックは安全である。

【００２５】

さらに、M_Key実行の指針は、現在のM_Key値を除いた全てのローカル状態情報についての読み取りのみのＳＭＰアクセスを可能とするように設定することができる。したがって、認証されていない（再）構成からスイッチベースのファブリックを保護することが可能であり、ホストベースのツールが発見操作および診断操作を行うことができる。

【００２６】

ＩＢアーキテクチャによってもたらされる柔軟性により、たとえばＨＰＣクラスタなどのＩＢファブリック／サブネットのアドミニストレータは、ファブリックにおいて１つ以上のスイッチに対して埋込型ＳＭインスタンスを使用するかどうか、および／またはＳＭ機能を実行するためにＩＢファブリックに対して１つ以上のホストを設定するかどうかを判定することができる。また、ＳＭによって使用されるＳＭＰによって定義されるワイヤープロトコルがＡＰＩを介して入手可能であることから、異なるツールおよびコマンドは、発見および診断のためのこのようなＳＭＰの使用に基づいて実施可能であり、また、現在のサブネットマネージャ操作とは独立して制御される。

【００２７】

セキュリティの観点から、ＩＢアーキテクチャの柔軟性は、ＩＢファブリックに接続された様々なホストへのルートアクセスとＩＢファブリック構成へのアクセスを可能とするルートアクセスとの間に基本的な違いがないことを示す。これは、物理的に安全で安定したシステムに関しては好適である。しかしながら、ＩＢファブリック上の異なるホストが異なるシステムアドミニストレータによって制御され、このようなホストがＩＢファブリック上で互いに論理的に隔離されるべきであるシステム構成に関しては、これは問題となり得る。

【００２８】

全てのコンポーネントの信頼性を常にファブリックに検証させる

本発明の実施形態によれば、ＩＢファブリックはそのコンポーネントの信頼性を常に検証することができる。サイトアドミニストレータは、システムにおける全てのＨＣＡの安全なファームウェアの状態を追跡し続けることができ、全ての関連するＨＣＡがセキュアモードで動作していることを簡単に信用することができる。さらに、信頼された個人によって正しいケーブル配線が確保される物理的に安全なデータセンタは、ファブリックにおける全てのコンポーネントの信頼性を保証することができる。加えて、サイト／ファブリックアドミニストレータは、帯域外管理インターフェイスが適切にパスワードで保護されていることを確実なものとすることができ、信用されるソフトウェアおよびファームウェアを信頼することができる。

【００２９】

上記の単純な手法は、適度な大きさの静的な構成には十分であるが、多数のノードもしくはコンポーネントを有する中くらいから大きい／非常に大きいサイズの動的環境には十分でない場合がある。認証処理を自動化するために、ファブリックコンポーネントは、ホストベースのスパイウェアまたは不明確な（不整合な）ホスト管理による影響を受けにくい態様で、コンポーネント自身、およびコンポーネントを制御するファームウェア／ソフトウェアのバージョンを認証することができるのが好ましい。

【００３０】

本発明の実施形態によれば、自動的なファブリックコンポーネント認証処理には、ピアが認証される前に秘密パスワードなどを送ることによってピアを含むことなくピア同士を互いに検証させることができる暗号化された要求／応答スキームの使用が伴う。ＩＢスイッチおよびＨＣＡファームウェアに関しては、ＳＭがデータトラフィックのためにポートを有効とする前にＳＭＰベースのプロトコルに伴って実施可能となる。

【００３１】

安全なＩＢファブリックにおいて、スイッチの信頼性は、第一にスイッチへの管理アクセスが安全であって、信頼されたサイト／ファブリックアドミニストレータのみがアクセスを行うことができるという前提の上に成り立っている。ＨＣＡの信頼性は、ひとたび物理的ホストが特殊なブート画像によって制御されるとＨＣＡが効果的にファブリックセキュリティドメインの一部となるという仮定に基づいて秘密キーを扱うことができるという特殊なホストブート画像ベースのスキームを使用して安全なものとすることができる。

【００３２】

発見されたコンポーネントの固有性を認証するための公開／秘密キーベースのスキーム

本発明の実施形態によれば、自動ファブリックコンポーネント認証処理は、秘密／公開キーのペアの使用に基づくことができる。

【００３３】

図２は、発明の実施形態に基づくＩＢファブリックにおいて発見されたコンポーネントを認証するための公開／秘密キーベースのスキームの使用を示す図である。図２に示されるように、ＩＢファブリック２００におけるＳＭ２０１は、ホスト２０３と関連付けられたＨＣＡ２０２などのファブリックコンポーネントを発見し、発見されたコンポーネントを認証する役割を担うことができる。ＳＭ２０１は、ＳＭ公開キー２１１およびＳＭ秘密キー２１２を保持し、これらは両方ともがＨＣＡ２０２を検証するための処理に使用される。

【００３４】
加えて、ＳＭ２０１は、ターゲットＨＣＡ２０２のためのＨＣＡ公開キー２１４など、認証されるべき各ターゲットコンポーネントのための公開キーを保持することができる。たとえばテナントに指定されたＨＣＡファームウェアバージョン２０４、ハイパーバイザ２０６／ＯＳ２０７など、ファブリックにおける各コンポーネントのための公開キーを記憶する中央レポジトリ２１０を設けてもよい。ある例において、特定のファームウェアバージョンまたはある範囲のファームウェアバージョンは、ファームウェアバージョン（または範囲）がリリース、インストール、または実行された場合に配信される、良好に規定された公開キーを有することができる。
【００３５】
さらに、ＨＣＡ２０２は、ＳＭ２０１側に記憶されている特定のＨＣＡ２０２のＨＣＡ公開キー２１４と関連付けられたＨＣＡ秘密キー２１３を保持することができる。ファブリックコンポーネントの信頼性は、関連するコンポーネントの秘密キーを注意深く配信することおよび記憶しておくことに依存する。一例としては、ＨＣＡの埋込型ファームウェアバイナリ２０４に隠されたＨＣＡ秘密キー２１３などの秘密キーを有することなどが挙げられる（すなわち、ＨＣＡバイナリの「逆アセンブル」で識別が非常に難しくなるような方法で）。追加の向上したスキームでは、タンパー防止不揮発性キー記憶部２０５など、出荷時の安定した記憶状態をより好適に利用することができる。
【００３６】
ＳＭ２０１、またはターゲットＨＣＡ２０２およびそのファームウェア２０４の完全性を制御する他のコンポーネントは、暗号化されたメッセージ２２１をＨＣＡファームウェア２０４に送信するように構成することができる。暗号化されたメッセージ２２１は、ＳＭインスタンスが所有するＳＭ公開キー２１１と併せてランダムバイトストリング２２０などのトークンを含むことができる。
【００３７】
暗号化されたメッセージ２２１を受信した後、要求を受けたＨＣＡファームウェア２０４は、受信した暗号化されたメッセージ２２１を復号化し、供給されたＳＭ公開キーを使用して暗号化された応答メッセージ２２２の形態でＳＭ２０１にランダムバイトストリング２２０を返信する。代替的に、受信した暗号化されたメッセージ２２１を復号化した後、要求を受けたＨＣＡファームウェア２０４は、ＳＭ２０１が異なるトークンの信頼性に注意を向けている限り、異なるバイトストリングなどの異なるトークンをＳＭ２０１に返信することができる。
【００３８】
そして、ＳＭ２０１は、所有する秘密キー２１２を使用して、受信したメッセージ２２２を復号化し、ＳＭ２０１が正しいバイトストリングを受信した場合にＨＣＡファームウェア２０４を認証することができる。したがって、偽のＨＣＡファームウェアまたはドライバの実装が同じセキュアバージョンＩＤを示すと主張し得るが、真のファームウェアバージョンの秘密キーが危殆化されていない限り、要求を通過させなくてもよい。
【００３９】
図３は、本発明の実施形態にかかるＩＢファブリックにおいて発見されたコンポーネントを認証するための公開／秘密キーに基づいた例示的なフローチャートを示す図である。図３に示されるように、ステップ３０１において、サブネットマネージャはまず第１の暗号化されたメッセージをＩＢファブリックにおけるファブリックコンポーネントに送信することができる。第１の暗号化されたメッセージは、トークンを含み、ファブリックコンポーネントと関連付けられた公開キーを使用して暗号化される。そして、ステップ３０２において、ファブリックコンポーネントは、ファブリックコンポーネントと関連付けられた秘密キーを使用して第１の暗号化されたメッセージを復号化することができるとともに、第２の暗号化されたメッセージをサブネットマネージャに返信することができる。最後に、ステップ３０３において、サブネットマネージャは、第２の暗号化されたメッセージが正しい情報を含む場合にファブリックコンポーネントを認証することができる。

【００４０】
本開示の教示によってプログラムされた１つ以上のプロセッサ、メモリ、および／またはコンピュータ読み取り可能な記憶媒体を含む１つ以上の従来の汎用もしくは専用デジタルコンピュータ、演算装置、マシン、またはマイクロプロセッサを使用し、本発明は都合よく実施され得る。適切なソフトウェアのコードは、ソフトウェア技術の当業者にとって明らかなように、本開示の教示に基づき、技能を有するプログラマーによって容易に準備され得る。
【００４１】
一部の実施形態において、本発明は、本発明の処理を実行するためにコンピュータをプログラミングするために使用することができる指令を記憶する記憶媒体またはコンピュータ読み取り可能な媒体（複数の媒体）であるコンピュータプログラム製品を含む。記憶媒体は、フロッピー（登録商標）ディスク、光ディスク、ＤＶＤ、ＣＤ－ＲＯＭ、マイクロドライブ、および光磁気ディスクを含む任意のタイプのディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＤＲＡＭ、ＶＲＡＭ、フラッシュメモリ装置、磁気もしくは光カード、ナノシステム（分子記憶ＩＣを含む）、または指令および／もしくはデータを記憶するのに適した任意のタイプの媒体もしくは装置を含み得るが、これらに限定されるものではない。
【００４２】
本発明の上記の実施形態は、例示および説明を目的として提供された。開示された形態そのものが本発明を網羅するものではなく、発明をこの形態に限定することを意図したものではない。多くの変更および変形が当業者にとって明らかである。実施形態は、発明およびその実施の原則を最良に説明するために選択および記載され、これによって当業者が様々な実施形態および考えられる特定の使用法に適した様々な変更について他の当業者が理解することができる。本発明の範囲が以下の請求項およびその均等物によって定義されることが意図される。

【図１】

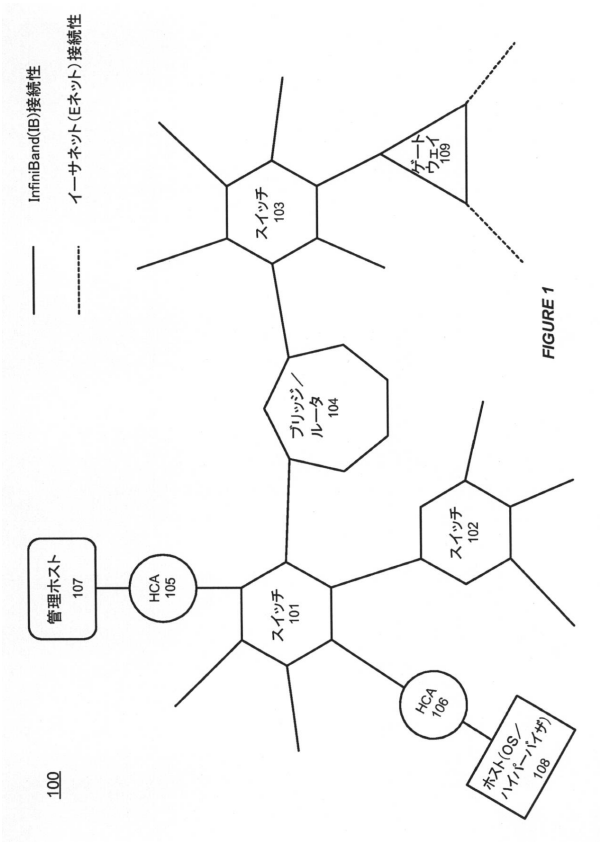

FIGURE 1

【図２】

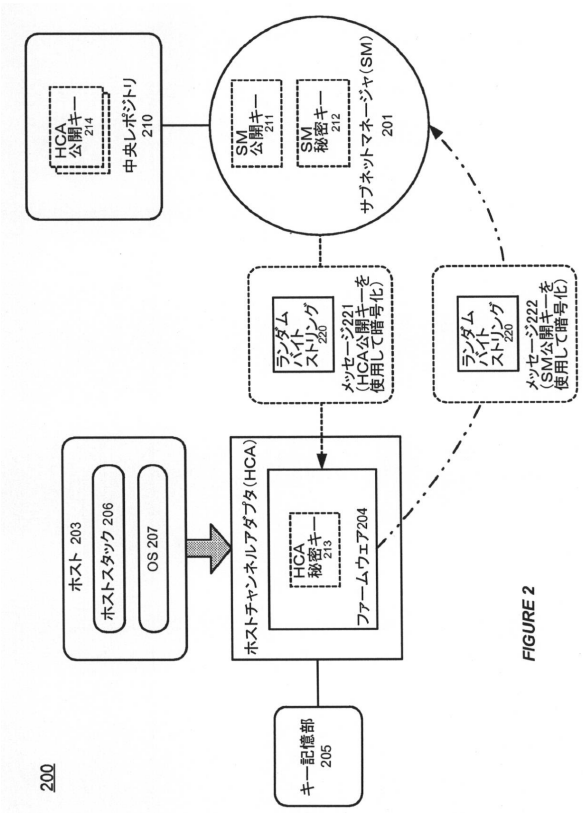

FIGURE 2

【図３】

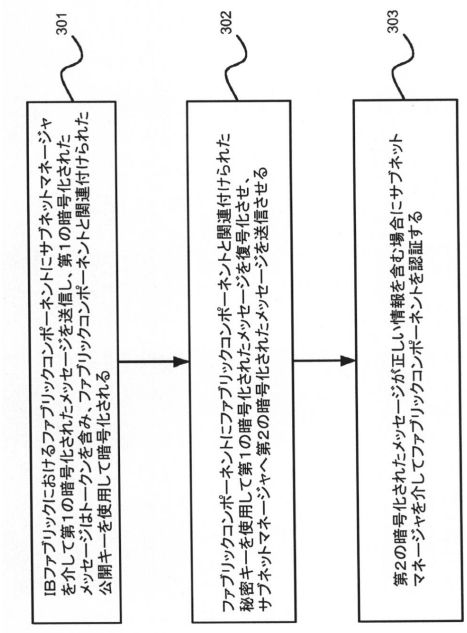

FIGURE 3

フロントページの続き

(72)発明者　トルドバッケン，オラ
ノルウェー、エヌ－０６７１　オスロ、ソラスベイエン、２３

審査官　平井　誠

(56)参考文献　米国特許第０７３９８３９４（ＵＳ，Ｂ１）
特表２００４－５２８６０９（ＪＰ，Ａ）
特表２００４－５２７１７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４４