(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7568206号
(P7568206)

(45)発行日　令和6年10月16日(2024.10.16)

(24)登録日　令和6年10月7日(2024.10.7)

(51)国際特許分類

Ｇ０６Ｆ　21/60　(2013.01)		Ｇ０６Ｆ	21/60	３６０
Ｈ０４Ｌ　9/10　(2006.01)		Ｈ０４Ｌ	9/10	Ａ

ＦＩ

請求項の数　6　（全15頁）

(21)出願番号　特願2022-542921(P2022-542921)
(86)(22)出願日　令和3年1月20日(2021.1.20)
(65)公表番号　特表2023-510002(P2023-510002A)
(43)公表日　令和5年3月10日(2023.3.10)
(86)国際出願番号　PCT/EP2021/051188
(87)国際公開番号　WO2021/148461
(87)国際公開日　令和3年7月29日(2021.7.29)
審査請求日　令和5年7月25日(2023.7.25)
(31)優先権主張番号　20461503.3
(32)優先日　令和2年1月20日(2020.1.20)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　522279483
ビットフォールド アーゲー
スイス国 カントン ズグ バール ６３４０ ミューレガッセ １８
(74)代理人　110000877
弁理士法人ＲＹＵＫＡ国際特許事務所
(72)発明者　ガンカルツ、カミル ラファル
ポーランド共和国、９５－１００ ズギェシ レンボウスキエゴ ６５／３３
審査官　塩澤 如正

最終頁に続く

(54)【発明の名称】　エアギャッピングハードウェアプロトコルを使用したセキュアなデータ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】

エアギャッピングを使用したセキュアなデータ転送のためのシステムであって、

第１のモジュールであって、

パブリックネットワークと通信するように構成された第１のモジュール通信インタフェース、ならびに、

前記パブリックネットワークからデータを送るように、かつ／または、受信するように構成された第１のモジュールコントローラおよび第１のモジュールデータインタフェースを有する第１のモジュールと、

第２のモジュールであって、

オペレーティングシステムを記憶している第１のリードオンリメモリ、

セキュリティ保護されたマシンまたはセキュリティ保護されたネットワークと通信して、前記第２のモジュールからデータを送信するように、また、前記第２のモジュールにデータを送信するように構成された第２のモジュール通信インタフェース、ならびに、

ブリッジモジュールと通信するためのマイクロコントローラおよび第２のモジュールデータインタフェースを有する

第２のモジュールと、

を備え、

前記ブリッジモジュールが、

ブリッジモジュールコントローラ、

前記ブリッジモジュールコントローラと通信するためのブリッジモジュールデータインタフェース、
データを記憶するためのメモリ、ならびに、
前記第１のモジュールデータインタフェースが前記第２のモジュールデータインタフェースに決して接続されないように、前記第１のモジュールデータインタフェースまたは前記第２のモジュールデータインタフェースに、選択的に前記ブリッジモジュールデータインタフェースを接続するように構成されたスイッチ、
を有し、
前記ブリッジモジュールコントローラが、前記第２のモジュールからデータを受信し、前記メモリに前記データを記憶し、前記データを前記第１のモジュールに送るように、かつ／または、前記第１のモジュールからデータを受信し、前記メモリに前記データを記憶し、前記データを前記第２のモジュールに送るように構成されており、
前記第２のモジュールが、
前記第２のモジュールの秘密鍵と、他の遠隔のエンティティの少なくとも１つの公開鍵とのセットを記憶している第２のリードオンリメモリ、ならびに、
前記第２のリードオンリメモリに記憶されている前記公開鍵および／または前記秘密鍵を使用して、データを暗号化および／または解読するように構成された暗号ユニット
を更に有する、
システム。
【請求項２】
前記スイッチが、単極双投（ＳＰＤＴ）スイッチである、
請求項１に記載のシステム。
【請求項３】
前記第１のモジュールおよび前記第２のモジュールが、共通の筐体内で、前記ブリッジモジュールと統合されている、
請求項１または２に記載のシステム。
【請求項４】
前記第２のモジュールデータインタフェースが、入力データバッファおよび出力データバッファを含む、
請求項１から３のいずれか一項に記載のシステム。
【請求項５】
請求項１から４のいずれか一項に記載のシステムを使用するエアギャッピングを使用したセキュアなデータ転送のための方法であって、
前記第２のモジュールにて、セキュアなデータを受信する段階と、
前記第２のモジュールにて、前記セキュアなデータを暗号化し、前記セキュアなデータに署名する段階と、
前記ブリッジモジュールの前記スイッチを前記第２のモジュールに切り替え、前記第２のモジュールから前記ブリッジモジュールに前記セキュアなデータを送る段階と、
前記ブリッジモジュールの前記スイッチを前記第１のモジュールに切り替え、前記ブリッジモジュールから前記第１のモジュールにデータを送る段階と、
前記第１のモジュールから前記パブリックネットワークを介して、指定された受信人にデータを送る段階と
を備える方法。
【請求項６】
請求項１から４のいずれか一項に記載のシステムを使用するエアギャッピングを使用したセキュアなデータ転送のための方法であって、
前記第１のモジュールにて、セキュアなデータを受信する段階と、
前記ブリッジモジュールの前記スイッチを前記第１のモジュールに切り替え、前記第１のモジュールから前記ブリッジモジュールに前記セキュアなデータを送る段階と、
前記ブリッジモジュールの前記スイッチを前記第２のモジュールに切り替え、データパ

ケットが権限を付与された当事者により署名されているかどうかを検証し、前記ブリッジモジュールから前記第２のモジュールにデータを送る段階と、
前記第２のモジュールにて、データをチェックし、解読する段階と、
前記セキュリティ保護されたマシンまたは前記セキュリティ保護されたネットワークに、前記第２のモジュールからデータを送る段階と
を備える方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、セキュリティ保護されたマシンまたはネットワーク（イントラネットなど）と、インターネットなどのパブリックネットワークとの間での、エアギャッピングハードウェアプロトコルを使用したセキュアなデータ転送のためのシステムおよび方法に関する。
【背景技術】
【０００２】
「エアギャッピング」は、あらゆるネットワーク接続からコンピューティングマシンを切り離した状態で維持すること、または、少なくともインターネットなどのパブリックネットワークからコンピューティングマシンを切り離した状態で維持することに関する周知の手順である。言い換えると、エアギャップ、エアウォールまたはエアギャッピングは、セキュリティ保護されていないネットワーク（パブリックインターネットまたはセキュリティ保護されていないローカルエリアネットワークなど）から、セキュアなコンピュータネットワークが物理的に分離されることを確実にするために１つまたは複数のコンピュータ上で用いられるネットワークセキュリティ対策である。
【０００３】
結果として、エアギャッピングを施されたコンピューティングマシンは、遠隔のエンティティがアクセス不可能であり、かつ、ユーザ（オペレータ）によって手動でのみ動作させることが可能な閉じたシステム（情報、信号などに関して閉じたシステム）である。
【０００４】
「Ｖｉｒｔｕａｌ　ａｉｒ　ｇａｐ　－　ＶＡＧ　ｓｙｓｔｅｍ」と題された米国特許第ＵＳ８９８４２７５Ｂ２号は、仮想エアギャップと、内部セキュリティコンポーネントと、外部セキュリティコンポーネントと、内部および外部セキュリティコンポーネントと共有メモリとの間に配置された、システムコンポーネントのメッセージ転送メカニズムとを備えるシステムを開示している。内部システムは、内部セキュリティコンポーネントと、システムに含まれ、システムを内部ネットワークに接続する他のコンポーネントとからなる。外部システムは、外部セキュリティコンポーネントと、システムに含まれ、システムを外部ネットワークに接続する他のコンポーネントとからなる。
【０００５】
米国特許出願第ＵＳ２０１９３７２７７９号は、ブロックチェーンへのアクセスを制御するために使用可能な秘密鍵などの情報のセキュアな記憶および取出しのための方法およびシステムであって、暗号資産保護システム内の複数の異なるヴォルトのうちのいずれかのヴォルトについてアクションを起こす要求を受け取ることであって、これらの複数の異なるヴォルトのそれぞれが、ヴォルト制御規則を規定する関連するポリシーマップを有する、受け取ることと、ハードウェアセキュリティモジュールにより制御される暗号鍵に基づいて、アクションが要求されているヴォルトについてのポリシーマップを、ハードウェアセキュリティモジュールにより認証することと、ヴォルトについてのポリシーマップがハードウェアセキュリティモジュールにより制御される暗号鍵に基づいて認証された場合に、ヴォルトについてのポリシーマップに突き合わせてアクションをチェックすることと、アクションがヴォルトについてのポリシーマップに従っていると確認された場合に、アクションを生じさせることとを含む方法およびシステムを開示している。
【発明の概要】
【０００６】

エアギャッピングの欠点は、エアギャッピングを施されたコンピューティングマシンと遠隔のエンティティとの間の情報の転送が、労力集約型であり、これにより、エアギャッピングを施されたマシンに入力されることが見込まれるソフトウェアアプリケーションまたはデータについての人間によるセキュリティ解析、また、場合によっては、セキュリティ解析後のデータの人間による手動での再入力さえ伴うことが多いということである。

【０００７】

さらに、エアギャッピングを施されたマシンは、一般に完全に分離されたハードウェアシステムであり、これは、２つのシステムを動作させ、維持することが必要であり、よって不便である。

【０００８】

上記に鑑みて、エアギャッピングを使用した、より便利でセキュアなデータ転送のためのシステムを設計することが必要である。

【０００９】

本発明は、エアギャッピングを使用したセキュアなデータ転送のためのシステムに関する。前記システムは、パブリックネットワークと通信するように構成された第１のモジュール通信インタフェース、ならびに、前記パブリックネットワークからデータを送るように、かつ／または、受信するように構成された第１のモジュールコントローラおよび第１のモジュールデータインタフェースを有する第１のモジュールを備える。前記システムは、第２のモジュールであって、オペレーティングシステムを記憶している第１のリードオンリメモリ、セキュリティ保護されたマシンまたはセキュリティ保護されたネットワークと通信して、前記第２のモジュールからデータを送信するように、また、前記第２のモジュールにデータを送信するように構成された第２のモジュール通信インタフェース、ならびに、ブリッジモジュールと通信するためのマイクロコントローラおよび第２のモジュールデータインタフェースを有する第２のモジュールを更に備える。また、前記システムは、ブリッジモジュールコントローラ、前記ブリッジモジュールコントローラと通信するためのブリッジモジュールデータインタフェース、データを記憶するためのメモリ、前記第１のモジュールデータインタフェースが前記第２のモジュールデータインタフェースに決して接続されないように、前記第１のモジュールデータインタフェースまたは前記第２のモジュールデータインタフェースに、選択的に前記ブリッジモジュールデータインタフェースを接続するように構成されたスイッチを有するブリッジモジュールを備え、前記ブリッジモジュールコントローラは、前記第２のモジュールからデータを受信し、前記メモリに前記データを記憶し、前記データを前記第１のモジュールに送るように、かつ／または、前記第１のモジュールからデータを受信し、前記メモリに前記データを記憶し、前記データを前記第２のモジュールに送るように構成されている。前記第２のモジュールは、前記第２のモジュールの秘密鍵と、他の遠隔のエンティティの少なくとも１つの公開鍵とのセットを記憶している第２のリードオンリメモリ、ならびに、前記第２のリードオンリメモリに記憶されている前記鍵を使用して、データを暗号化および／または解読するように構成された暗号ユニットを更に有する。

【００１０】

前記スイッチは、単極双投（ＳＰＤＴ）スイッチであり得る。

【００１１】

前記第１のモジュールおよび前記第２のモジュールは、共通の筐体内で、前記ブリッジモジュールと統合され得る。

【００１２】

前記第２のモジュールデータインタフェースは、入力データバッファおよび出力データバッファを含み得る。

【００１３】

また、本発明は、上記のようなシステムを使用するエアギャッピングを使用したセキュアなデータ転送のための方法に関し、前記方法は、前記第２のモジュールにて、セキュアなデータを受信する段階と、前記第２のモジュールにて、前記セキュアなデータを暗号化

し、前記セキュアなデータに署名する段階と、前記ブリッジモジュールの前記スイッチを前記第２のモジュールに切り替え、前記第２のモジュールから前記ブリッジモジュールに前記セキュアなデータを送る段階と、前記ブリッジモジュールの前記スイッチを前記第１のモジュールに切り替え、前記ブリッジモジュールから前記第１のモジュールにデータを送る段階と、前記第１のモジュールから前記パブリックネットワークを介して、指定された受信人にデータを送る段階とを備える。

【００１４】

前記方法は、前記第１のモジュールにて、セキュアなデータを受信する段階と、前記ブリッジモジュールの前記スイッチを前記第１のモジュールに切り替え、前記第１のモジュールから前記ブリッジモジュールに前記セキュアなデータを送る段階と、前記ブリッジモジュールの前記スイッチを前記第２のモジュールに切り替え、データパケットが権限を付与された当事者により署名されているかどうかを検証し、前記ブリッジモジュールから前記第２のモジュールにデータを送る段階と、前記第２のモジュールにて、データをチェックし、解読する段階と、前記セキュリティ保護されたマシンまたは前記セキュリティ保護されたネットワークに、前記第２のモジュールからデータを送る段階とを更に備え得る。

【００１５】

本発明のこれらの特徴、態様および利点、ならびに、他の特徴、態様および利点が、以下での図面、説明および特許請求の範囲を参照することでより良好に理解されるようになるであろう。

【図面の簡単な説明】

【００１６】

本明細書で提示されるこれらの目的および他の目的は、エアギャッピングハードウェアプロトコルを使用したセキュアなデータ転送のためのシステムおよび方法を提供することで実現される。本開示の更なる詳細および特徴、それらの特性、ならびに、様々な利点が、図に示される好ましい実施形態の以下での詳細な説明からより明らかになるであろう。

【００１７】

【図１】セキュリティ保護されていないネットワークに接続された、本明細書で提示されるシステムの第１のモジュールの図である。

【図２】セキュリティ保護されたマシンまたはセキュリティ保護されたネットワークに接続された、本明細書で提示されるシステムの第２のモジュールの図である。

【図３】第１のモジュールと第２のモジュールとの間で動作しているブリッジモジュールを示す図である。

【図４】第１のモジュール、第２のモジュール、およびブリッジを備えるシステムの概要を示す図である。

【図５】セキュリティ保護された環境からデータを送るためのセキュアなデータ転送の方法を示す図である。

【００１８】

【図６】セキュリティ保護された環境へのデータを受信するためのセキュアなデータ転送の方法を示す図である。　［表記および用語］

【００１９】

以下の詳細な説明のいくつかの部分は、コンピュータメモリ上で実行され得る、データビットに対する動作からなるデータ処理手順、段階または他の記号表現に関して提示されている。したがって、コンピュータは、そのような論理段階を実行するので、物理量の物理操作を必要とする。

【００２０】

これらの量は通常、コンピュータシステム内で記憶すること、転送すること、組み合わせること、比較すること、そうでなければ操作することが可能な電気信号または磁気信号の形態を取る。慣用上の理由で、これらの信号は、ビット、パケット、メッセージ、値、エレメント、シンボル、キャラクタ、ターム、またはナンバなどと称される。

【００２１】

さらに、これらの用語および同様の用語の全ては、適当な物理量に関連するべきものであり、これらの量に適用される便利なラベルに過ぎない。例えば、「処理」または「作成」または「転送」または「実行」または「決定」または「検出」または「取得」または「選択」または「計算」または「生成」などの用語は、コンピュータシステムであって、そのコンピュータのレジスタおよびメモリ内で物理（電子）量として表されているデータを操作し、そのデータを、メモリもしくはレジスタまたは他のそのような情報ストレージ内で物理量として同様に表される他のデータに変換するコンピュータシステムのアクションおよび処理を指す。

【００２２】

一般に、本明細書で参照されるもののようなコンピュータ可読（記憶）媒体は、非一時的なものであってもよく、かつ／または、非一時的デバイスを備えてもよい。この文脈において、非一時的記憶媒体は、有形であり得るデバイスを含んでよい。これは、当該デバイスが具体的な物理形態を有するが、当該デバイスがその物理状態を変え得ることを意味する。したがって、例えば、非一時的とは、状態が変化しても有形のままであるデバイスを指す。

【００２３】

本明細書では、「例」という用語は、非限定的な例、事例または例示としての役割を果たすことを意味する。本明細書では、「例えば（ｆｏｒ　ｅｘａｍｐｌｅ）」という用語および「例えば（ｅ．ｇ．）」という用語は、１つまたは複数の非限定的な例、事例または例示の一覧を紹介する。

【発明を実施するための形態】

【００２４】

以下の詳細な説明は、本発明を実施するモードであって、現在のところ企図されている最善のモードの説明である。この説明は、限定を行う意味で解釈されるべきではなく、本発明の一般原則を説明する目的のみのものである。

【００２５】

図４に示すような全体構造を有する本明細書で提示されるシステムは、特に、セキュリティ保護されたマシンまたはセキュリティ保護されたネットワーク（第２のモジュール２００が接続されている）と、インターネット（第１のモジュール１００が接続されている）などのパブリックネットワーク、ＬＡＮカード、または、それと同様の通信モジュールを介して接続された指定された受信人との間での、効率的かつ便利で急速なセキュアなデータ転送を提供するように構成することが可能である。

【００２６】

本システムは、極秘データを処理する設備を接続するパブリックネットワークを介した極秘データの転送に特に有用である。例えば、ある製造会社は、特定の商品を製造する複数の工場と、各工場での製造プロセスに関する極秘データを集める中央ハブとを有することがある。そのケースでは、製造データをシステム４００を介して送信することができ、極秘データを生成するマシンが、第２のモジュール２００に接続されており、第２のモジュール２００は、パブリックネットワークに対してエアギャッピングを施されており、中央ハブにデータを送ること、および／または、中央ハブからデータを受信することが必要なケースでのみ、パブリックネットワークにセキュアに接続される。さらに、ほとんどのケースでは、製造会社は、自体の設備のセキュアなＩＴ環境がハッキングされるリスクのせいで、インターネットまたは公に利用可能な他のネットワークに設備を接続するリスクを冒すことができない。本明細書で説明されるデバイスは、権限を付与されていないエンティティ（例えば、ハッカー）がセキュリティ保護されたネットワークまたはセキュリティ保護されたマシン内に接続することをエアギャッピングにより阻止する。本明細書で説明されるシステムは、権限を付与されたエンティティのデジタル暗号鍵で署名されたセキュリティ保護された通信の転送のみを可能にする。さらに、本明細書で説明されるシステムは、別々の場所にあり、インターネットを介して接続してペアにされる上記の２つのマシンを介したセキュアな通信に使用することが可能である。

【００２７】
本デバイスの他の用途は、宇宙衛星などの専門化されたエンティティとのセキュアな通信のためのものであり、権限を付与されていないエンティティによるアクセスを阻止することが最も重要である。
【００２８】
本システムは、専用コンポーネントまたは特注のＦＰＧＡ（フィールドプログラマブルゲートアレイ）回路もしくはＡＳＩＣ（特定用途向け集積回路）回路を使用して実現することができる。
【００２９】
図１は、本システムの第１のモジュール１００の図を示す。第１のモジュール１００は、ＴＣＰ／ＩＰなどの一般的なプロトコルにより、一般的なネットワーク（ＬＡＮ）カードなどを介してインターネット（または、一般には任意の非セキュアなパブリックネットワーク）に接続される。第１のモジュール１００は、セキュリティ保護されたシステムからデータを受信すること、または、セキュリティ保護されたシステムにデータを送ることに関係する権限を付与された任意の外部の当事者との通信を担う。換言すると、それは通信モジュールである。
【００３０】
第１のモジュール１００は、システムの他のコンポーネントに通信可能に結合されるデータバス１０１を備え、これにより、それらのコンポーネントを、第１のモジュールコントローラ１０５により効果的に管理することができる。
【００３１】
フラッシュメモリ１０４は、下記で説明される方法の段階を実行するために第１のモジュールコントローラ１０５により実行される１つまたは複数のコンピュータプログラムを記憶することができる。さらに、フラッシュメモリ１０４は、第１のモジュール１００の構成パラメータを記憶することができる。
【００３２】
第１のモジュール通信インタフェース１０２は、ＴＣＰ／ＩＰプロトコルを使用するＬＡＮカード、または、他の通信インタフェース（例えば、Ｗｉ－Ｆｉ（登録商標）、ＧＳＭ（登録商標）、３Ｇ、ＬＴＥ、もしくは５Ｇなど）であり得、外部のパブリックネットワークとの通信を管理するように構成される。第１のモジュール通信インタフェース１０２は、その動作をユーザが自分自身で制御することができるように専用のオン／オフ・スイッチを有し得る。
【００３３】
第１のモジュールコントローラ１０５は、ランダムアクセスメモリ（ＲＡＭ）１０５Ａと、フラッシュメモリ１０５Ｃに記憶された命令により指定される基本的な算術演算、論理演算、制御動作、および、入出力（Ｉ／Ｏ）動作を実行することによりコンピュータプログラムの命令を実行するコンピュータ内の電子回路である中央処理ユニット（ＣＰＵ）１０５Ｂと、第１のモジュール１００の他のコンポーネントからのデータの受信、および／または、それらへのデータの送信を担うデータインタフェース１０５Ｄとを備えるシステムオンチップであり得る。
【００３４】
一般に、第１のモジュール１００は、第１のモジュール通信インタフェース１０２を介して、遠隔のサーバまたはクライアント（例えば、工場から極秘データを集めるか、または、製造設備に命令を送る製造会社の中央ハブ）との通信を確立するように構成される。
【００３５】
例えば、イーサネット（登録商標）を介したＴＣＰ／ＩＰ技術を使用してデータバス１０１へのアクセスを可能にする第１のモジュールデータインタフェース１０６を介して、モジュール１００とモジュール３００との間でデータを暗号化された形態で送信することが可能である。
【００３６】

図２は、本明細書で提示されるシステムの第２のモジュール２００の図を示す。第２のモジュール２００は、ＴＣＰ／ＩＰまたはこれに類似したプロトコルを使用して、ＬＡＮカードまたは他のネットワーク接続を介することで、セキュリティ保護されたマシンとの通信、または、極秘データの生成または受信を行い、パブリックネットワーク（インターネットなど）に決して接続されない（または、第１のモジュール１００が接続されているいずれのネットワークにも接続されない）セキュリティ保護されたネットワーク（イントラネットなど）（ただし、当該ネットワークは、第２のモジュール２００に結合されているセキュリティ保護されたネットワークまたはセキュリティ保護されたマシンに接続されている）との通信を担う。

【００３７】

第２のモジュールは、そのモジュールの要素を通信可能に結合するデータバス２０１を備える。

【００３８】

第１のリードオンリメモリ２０２（ＲＯＭ）は、第２のモジュール２００のオペレーティングシステムを記憶する（このオペレーティングシステムは、ＲＯＭに記憶されているので改変されない）。

【００３９】

システムのコンポーネントは、データバス２０１に通信可能に結合され、これにより、それらを、マイクロコントローラ２０５により管理することができる。

【００４０】

ファイル、ウイルスなどを送ること、または、第２のモジュールに探りを入れることに基づくハッキングの試みをエアギャップにより阻止することなどのために、第２のリードオンリメモリ２０３（ＲＯＭ）は、例えばインターネットなどのセキュリティ保護されていないネットワークから受信されるメッセージおよび命令を有効化するための認証鍵を記憶する。具体的には、第２のリードオンリメモリ２０３は、受信されたデータに署名する、およびそれを解読するための、第２のモジュール２００に関連する秘密鍵と、データの受信人または送信元の公開鍵（それぞれ異なる受信人または送信元にデータを送ることが可能な場合は複数の鍵）であって、データが受信人によってのみ読み取ることが可能なようにデータを暗号化するための、または、データの受信されたパケットの信頼性を確認するための（ハッカーからの保護）公開鍵とを記憶する。

【００４１】

セキュリティを高めるために、ＲＯＭ２０２とＲＯＭ２０３との両方は、鍵および／またはオペレーティングシステムの定期的な物理的アップデートを容易にするように、容易に置換えができるように構成することができる。

【００４２】

フラッシュメモリ２０４は、極秘データを暗号化（データを送り出す場合）または解読（データが受信された場合）するために記憶するように構成される。

【００４３】

マイクロコントローラ２０５は、デバイスの機能を制御するように、具体的には、図５および図６で説明されるセキュアなデータ転送の方法を指揮するように使用される。さらに、マイクロコントローラ２０５は、第２のモジュール２００のコンポーネントに追加の機能を提供するように使用することもできる。マイクロコントローラ２０５は、プロセッサ２０５Ａと、オペレーティングＲＡＭメモリ２０５Ｂと、内部フラッシュメモリ２０５Ｃとを備えることができる。

【００４４】

セキュアなデータを生成または受信するセキュリティ保護されたシステムと通信するために、第２のモジュール通信インタフェース２０８が使用される。例えば、第２のモジュール通信インタフェース２０８は、セキュリティ保護されたシステムまたはイントラネットなどのセキュリティ保護されたネットワークのＰＬＣコントローラと通信するように構成されるイーサネットインタフェースであり得る（第２のモジュール通信インタフェース

２０８は、ＴＣＰ／ＩＰプロトコルを使用することができる）。
【００４５】
第２のＲＯＭ２０３に記憶された鍵を使用して極秘データを暗号化および／または解読するように、暗号ユニット２０９が使用される。暗号ユニット２０９は、暗号化／解読アルゴリズムを急速に実行可能なＦＰＧＡ回路の形態を有することが好ましい。
【００４６】
モジュール２００とモジュール３００との間で、第２のモジュールデータインタフェースを介してデータを送信することが可能であり、第２のモジュールデータインタフェースは、ＳＰＤＴスイッチ３１０を介してブリッジモジュールインタフェース３０９と通信するように構成されるデータバッファ２０６、２０７の形態であることが好ましい。入力バッファ２０６は、そこからデータを読み取るために第２のモジュールがアクセス可能であり、それにデータを記憶するためにブリッジモジュールがアクセス可能である。出力バッファ２０７は、それにデータを記憶するために第２のモジュールがアクセス可能であり、そこからデータを読み取るためにブリッジモジュールがアクセス可能である。データバッファ２０６、２０７のそれぞれは、自体の内部処理ユニットと、フラッシュメモリと、データバス２０１との通信、ならびに、ＳＰＤＴスイッチ３１０を介したブリッジモジュールデータインタフェース３０９との通信に対処するためのデータインタフェースとを備えることができる。さらに、入力バッファ２０６は、ＲＯＭ２０３内に記憶された公開鍵とペアにされた適切な秘密鍵でデータが署名されていない場合には、データパケットを第２のモジュール２００の内部に渡すことができないので、入力バッファ２０６は、権限を付与されていないエンティティ（例えば、ハッカー）による侵害から、第２のモジュール２００のセキュアな環境を保護し、この結果、そのモジュールに接続されたセキュリティ保護されたネットワークまたはマシンも保護することになる。
【００４７】
第２のモジュール２００は、専用のコンポーネントまたは特注のＦＰＧＡ回路もしくはＡＳＩＣ回路を使用して実現することができる。
【００４８】
ブリッジモジュール３００とともに第２のモジュール２００を共通の筐体内で統合して、イーサネットインタフェースなどの外部インタフェースを介して、第１のモジュールに接続可能（ブリッジモジュールを介してのみ）な専用のデバイスを形成することが可能である。モジュール１００、２００、３００の全てを共通の筐体内で統合して、完全に機能的なデバイスを形成することができることが好ましい。
【００４９】
図３は、第１のモジュール１００と第２のモジュール２００との間で動作するブリッジモジュール３００を示す。ブリッジモジュール３００の目的は、第２のモジュール２００から第１のモジュール１００に、かつ／または、第１のモジュール１００から第２のモジュール２００にセキュアなデータをセキュアに渡すことである。
【００５０】
ブリッジモジュール３００は、専用のコンポーネントまたは特注のＦＰＧＡ回路もしくはＡＳＩＣ回路を使用して実現することができる。
【００５１】
ブリッジモジュール３００は、スイッチを介して送信されるデータを記憶するためのフラッシュメモリなどのメモリ３０３に通信可能に結合されるデータバス３０１を備える。さらに、システムの他のコンポーネントが、データバス３０１に通信可能に結合され、これにより、それらを、ブリッジモジュールコントローラ３０５により管理することができる。
【００５２】
第１のモジュール１００とブリッジ３００との間で、または、第２のモジュール２００とブリッジ３００との間で所与の時間にデータを送信することが可能である。最大限のセキュリティのために、システムは、データの送信を制御するＳＰＤＴスイッチ３１０を使

用することで、いつであっても、３つのモジュール１００、２００、３００の全てが同時にアクティブになることができないように構成される。

【００５３】

ブリッジモジュールコントローラ３０５は、マイクロコントローラであっても、または、マイクロコントローラもしくはそれに類似するサブコンポーネントを、第１のモジュールコントローラ１０５として備えるシステムオンチップモジュールであってもよく、ディスプレイ３０６上での情報の表示を制御するためのグラフィック処理ユニットを有してもよいが、このことは必須ではない。

【００５４】

オン／オフ・スイッチ３０４が、ユーザにより動作させられた際にデバイスをオンまたはオフに切り替えるように構成される。他の典型的なコンポーネントは、ディスプレイ３０６、入力インタフェース３１１（簡易型キーボードまたは小数のみのキーなど）を含み、ユーザとの通信のためのコンポーネントを形成するスピーカ３０２を有してもよい。

【００５５】

ブリッジモジュール３００は、モジュール３０７により電力を供給され、モジュール３０７は、電源に接続される電力供給部であってもよく、または、パワーオーバイーサネット技術を使用した電力供給部であってもよい。

【００５６】

ブリッジモジュール３００は、ブリッジまたは第１のモジュールのプログラミング（または構成）を可能にするためのプログラミングポート３１２（ＵＳＢ、イーサネット、または、ＲＳ２３２など）を更に備えることができる。

【００５７】

ブリッジモジュール３００は、第１のモジュールインタフェース１０６と、または、第２のモジュール２００のデータバッファ２０６、２０７と、両者ともにＳＰＤＴスイッチ３１０を介して通信するように構成されるブリッジモジュールデータインタフェース３０９を備える。ブリッジモジュールデータインタフェース３０９は、データバス３０１を介して、または、専用の接続線を介して直接的にＳＰＤＴスイッチに接続することができる。

【００５８】

ＳＰＤＴ（単極双投）スイッチモジュール３１０は、１度にモジュールのうちの１つのみに（第１のモジュール１００または第２のモジュール２００に）データを送信することが可能なように構成される。

【００５９】

第１のモジュールデータインタフェース１０６が第２のモジュール２００のデータバッファ２０６、２０７に決して接続されないという機能が提供される限り、ＳＰＤＴスイッチの代わりに他の種類のスイッチングモジュールを使用してもよい。

【００６０】

図４は、第１のモジュール１００と、第２のモジュール２００と、ブリッジモジュール３００とを備えるシステムであって、ブリッジモジュール３００が、所与の時間にＳＰＤＴスイッチ３１０を介して第１のモジュール１００または第２のモジュール２００に選択的に接続される、システムの概要を示す。ＳＰＤＴスイッチ３１０は、データの送信を制御する。

【００６１】

したがって、システム４００は、少なくとも３つのモジュール、すなわち、第１のモジュール１００と、第２のモジュール２００と、モジュール１００とモジュール２００との間でデータを渡すことを可能にし、モジュール１００およびモジュール２００が互いから独立して動作することを可能にするブリッジモジュール３００とに分割されることでセキュリティ問題を解決することが可能である。第２のモジュール２００は、セキュリティ保護されたマシンまたはネットワークをウイルスおよびハッカーによる侵害から保護するために、パブリックネットワーク（インターネットなど）に決して接続されることなく、自体の秘密鍵または受信人の公開鍵を使用してセキュアなデータを暗号化するように、また

、セキュリティ保護されていないネットワークから、セキュリティ保護された（かつ暗号化された）メッセージおよび命令を、それらを有効化（および解読）する方法を用いて受信するように構成される。

【００６２】

具体的には、所与の事例のいずれにおけるブリッジモジュール３００も、第１のモジュール１００と第２のモジュール２００とのいずれかに接続することが可能であるで、第２のモジュール２００は、パブリックネットワークまたはセキュリティ保護されていない他のネットワークに決して接続されない。したがって、遠隔のエンティティ（ハッカーまたはスパイソフトウェアを動作させるマシン）が、第２のモジュール２００に直接的にアクセスを試みることは不可能である。第１のモジュール１００もまた、第２のモジュール２００または第２のモジュール２００に接続されたネットワークのデータまたは内容にアクセスするための形態を何ら有さない。

【００６３】

図５および図６のセキュアなデータ転送の方法を参照してデバイスの機能を説明する。これらの方法は、マイクロコントローラ２０５が指揮することが可能である。

【００６４】

図５は、第２のモジュールからパブリックネットワークを介して、指定された受信人にデータを送るためのセキュアなデータ転送の方法を示す。まず、段階５０１で、第２のモジュールがオンに切り替えられ、ブリッジのＳＰＤＴスイッチが、第２のモジュールの２０７直接出力バッファに設定される。

【００６５】

一般には、デバイスの動作中に、第１のモジュール１００および第２のモジュール２００の両方をオンにすること、または、モジュール１００、２００のうちの１つのみをオンにする（潜在的にセキュリティをより高くするために）ことができる。

【００６６】

あるいは、第２のモジュール２００が、第２のモジュール２００に接続されているセキュリティ保護されたネットワークまたはセキュリティ保護されたマシンからデータを受信し、次いでそれを暗号化している際には、ＳＰＤＴスイッチを第１のモジュール１００に接続することも可能であるが、既に暗号化されているデータをブリッジモジュール３００に転送して、更にデータ転送を進めるためには、ＳＰＤＴスイッチを第２のモジュール２００に接続することが必要である。

【００６７】

次に、段階５０２で、セキュアなデータが第２のモジュールにより受信される。次いで、段階５０３で、セキュアなデータが暗号化され署名される（データが送信されるべき受信人の公開鍵を使用して暗号化され、第２のモジュールの秘密鍵により署名される）。次に、段階５０４で、暗号化されたデータが、第２のモジュールからブリッジモジュールに送られる。データが受信され、ブリッジモジュールのメモリに記憶された後、段階５０５で、ＳＰＤＴスイッチが第１のモジュールに設定され、段階５０６で、ブリッジモジュールから第１のモジュールにデータが送られる。続いて、段階５０７で、第１のモジュールからパブリックネットワークを介して、指定された受信人にデータが送られる。

【００６８】

図６は、パブリックネットワークから第２のモジュールによりデータを受信するためのセキュアなデータ転送の方法を示す。まず、段階６０１で、第１のモジュールがオンに切り替えられ、ブリッジのＳＰＤＴスイッチが、第１のモジュールに設定される。

【００６９】

あるいは、パブリックネットワークからのデータの受信中には、ＳＰＤＴスイッチを第２のモジュール２００に接続することも可能であるが、データをブリッジモジュール３００に転送して、データ転送に伴い更に処理するためには、ＳＰＤＴスイッチを第１のモジュール１００に接続することが必要である。

【００７０】

一般には、デバイスの動作中に、第１のモジュール１００および第２のモジュール２００の両方をオンにすること、または、モジュール１００、２００のうちの１つのみをオンにする（潜在的にセキュリティをより高くするために）ことができる。

【００７１】

次に、段階６０２で、データが第１のモジュールにより受信される。次いで、段階６０３で、第１のモジュールからブリッジモジュールにデータが送られる。データが受信され、ブリッジモジュールのメモリに記憶された後、段階６０４で、ＳＰＤＴスイッチは、第２のモジュールの２０６直接入力バッファに設定され、ＲＯＭ２０３および２０６直接入力バッファのコンピューティングユニットに記憶された暗号鍵のセットを使用して、権限を付与された当事者によりデータが署名されているか、データが第２のモジュールに入ることが可能かについてデータが検証され、そうであると検証されれば、段階６０５で、データはブリッジモジュールから第２のモジュールに転送される。続いて、段階６０６で、第２のモジュールにてデータがチェックおよび解読される。こうして初めて、段階６０７で、展開および解読されたデータが第２のモジュールからセキュリティ保護されたマシンまたはセキュリティ保護されたネットワークに送られる。

【００７２】

提示された方法およびシステムは、使用性を損なうことなく電子的データ送信のセキュリティを改善することを可能にする。したがって、それらは、有用、具体的かつ有形の結果を提供する。機械・変換テストは満たされており、思想は抽象的ではない。

【００７３】

本明細書で開示される方法の少なくとも一部分を、コンピュータ実装することもできる。したがって、本システムは、完全にハードウェアの実施形態、完全にソフトウェアの実施形態（ファームウェア、常駐ソフトウェア、マイクロコードなどを含む）、または、本明細書では概して「回路」、「モジュール」、もしくは、「システム」と全て称することができる、ソフトウェアの側面とハードウェアの側面とを組み合わせた実施形態の形を取ることができる。

【００７４】

さらに、本システムは、任意の有形の表現媒体であって、コンピュータ使用可能プログラムコード（量子コンピューティングソフトウェアが含まれる）がその媒体内で具現化される、有形の表現媒体内で具現化されるコンピュータプログラム製品の形態を取ることができる。

【００７５】

エアギャップを介したセキュアなデータ転送のための前述の方法は、１つまたは複数のコンピュータプログラムにより実行および／または制御することができることを当業者であれば容易に理解することが可能である。そのようなコンピュータプログラムは、典型的には、コンピューティングデバイス内のコンピューティングリソースを利用することにより実行される。アプリケーションが非一時的媒体に記憶される。非一時的媒体の例は、例えばフラッシュメモリなどの不揮発性メモリであるが、揮発性メモリの例はＲＡＭである。コンピュータ命令は、プロセッサにより実行される。これらのメモリは、本明細書において提示される技術的概念によるコンピュータ実装方法の全ての段階を実行するコンピュータ実行可能命令を含むコンピュータプログラムを記憶するための例示的な記録媒体である。

【００７６】

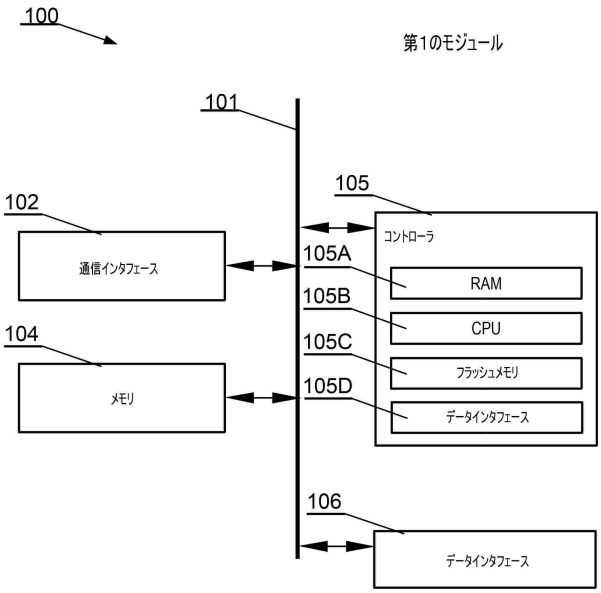
特定の好ましい実施形態を参照して、本明細書において提示されるシステムおよび方法の図示、説明、および、定義を行ったが、前述の明細書における実装形態のそのような参照および例は、当該方法または当該システムに対するいかなる限定も示唆しない。しかしながら、技術的概念のより広い範囲から逸脱することなく、それらに対して様々な修正および変更が行われ得ることは明らかであろう。提示された好ましい実施形態は、例示的なものに過ぎず、本明細書において提示された技術的概念の範囲を網羅したものではない。

【００７７】

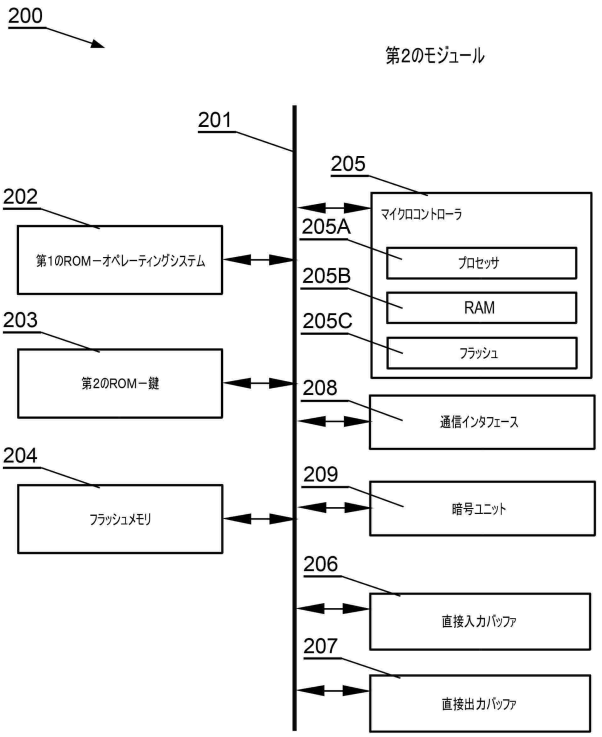
したがって、保護範囲は、本明細書において説明した好ましい実施形態に限定されず、以下の特許請求の範囲によってのみ限定される。

【図面】

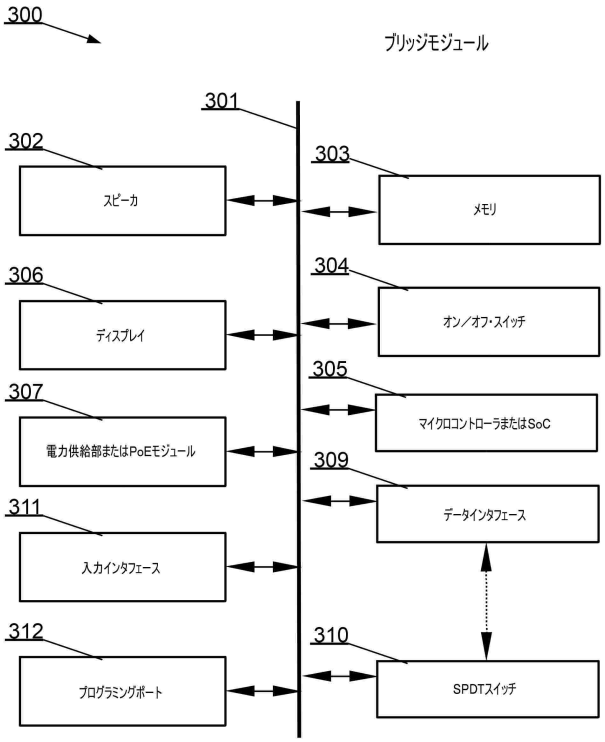
【図１】



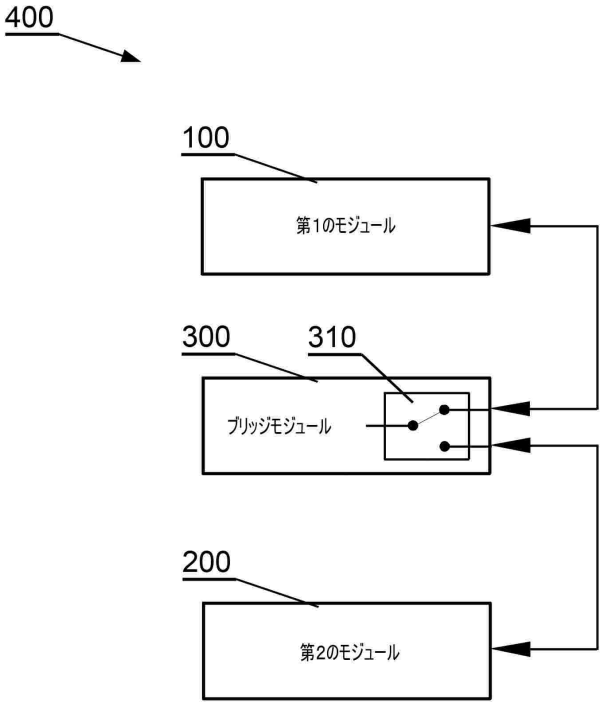
【図２】



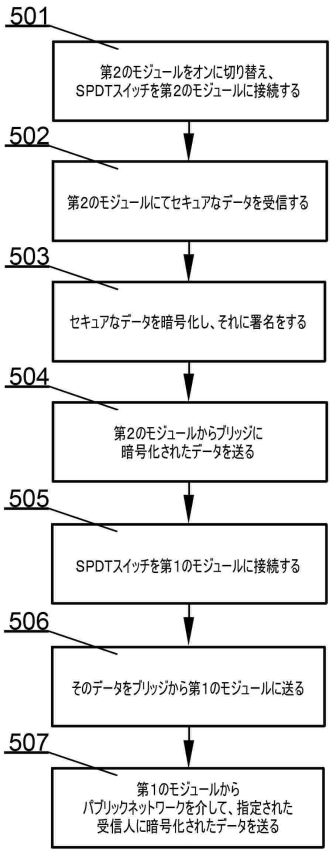
【図３】



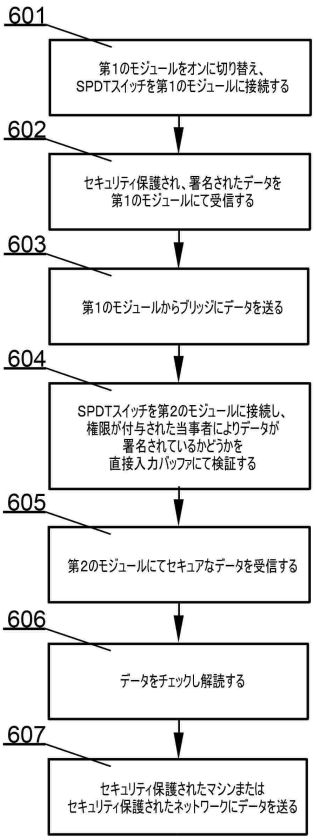
【図４】



【図５】


501
第2のモジュールをオンに切り替え、
SPDTスイッチを第2のモジュールに接続する
502
第2のモジュールにてセキュアなデータを受信する
503
セキュアなデータを暗号化し、それに署名をする
504
第2のモジュールからブリッジに
暗号化されたデータを送る
505
SPDTスイッチを第1のモジュールに接続する
506
そのデータをブリッジから第1のモジュールに送る
507
第1のモジュールから
パブリックネットワークを介して、指定された
受信人に暗号化されたデータを送る

【図６】


601
第1のモジュールをオンに切り替え、
SPDTスイッチを第1のモジュールに接続する
602
セキュリティ保護され、署名されたデータを
第1のモジュールにて受信する
603
第1のモジュールからブリッジにデータを送る
604
SPDTスイッチを第2のモジュールに接続し、
権限が付与された当事者によりデータが
署名されているかどうかを
直接入力バッファにて検証する
605
第2のモジュールにてセキュアなデータを受信する
606
データをチェックし解読する
607
セキュリティ保護されたマシンまたは
セキュリティ保護されたネットワークにデータを送る

フロントページの続き

(56)参考文献　　米国特許出願公開第２０１９／０３７２７７９（ＵＳ，Ａ１）
特表平１１－５０２９７６（ＪＰ，Ａ）
特表２０１４－５０１９５５（ＪＰ，Ａ）
特開２００５－３０９７５８（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　　９／１０