

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-169190

(P2017-169190A)

(43) 公開日 平成29年9月21日 (2017.9.21)

(51) Int.Cl.	F I	テーマコード (参考)
HO4L 9/32 (2006.01)	HO4L 9/00 675B	5B042
HO4L 9/08 (2006.01)	HO4L 9/00 601F	5J104
HO4M 11/00 (2006.01)	HO4M 11/00 302	5K201
HO4M 3/00 (2006.01)	HO4M 3/00 E	
GO6F 11/30 (2006.01)	GO6F 11/30 158	

審査請求 未請求 請求項の数 19 O L 外国語出願 (全 23 頁) 最終頁に続く

(21) 出願番号 特願2016-244456 (P2016-244456)
 (22) 出願日 平成28年12月16日 (2016.12.16)
 (31) 優先権主張番号 14/971, 806
 (32) 優先日 平成27年12月16日 (2015.12.16)
 (33) 優先権主張国 米国 (US)

(特許庁注：以下のものは登録商標)

1. SMALLTALK

(71) 出願人 509233459
 フルークコーポレイション
 Fluke Corporation
 アメリカ合衆国、ワシントン州 98203、エバレット、シーウェイブールバード 6920
 6920 Seaway Boulevard, Everett, Washington 98203 U. S. A.

(74) 代理人 110001209
 特許業務法人山口国際特許事務所
 (72) 発明者 ジョン・ポール・ヒッテル
 アメリカ合衆国 アリゾナ州 85254
 スコットズデイル イースト エア・リーブル・アヴェニュー 5202

最終頁に続く

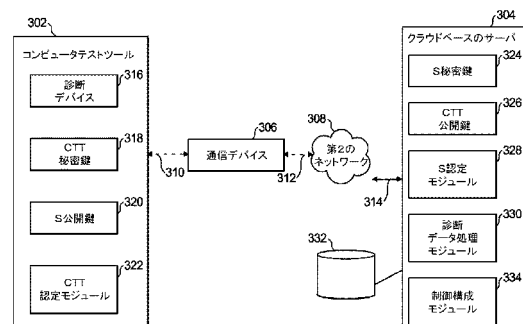
(54) 【発明の名称】 コンピュータテストツールとクラウドベースのサーバとの間の安全な通信のためのシステム及び方法

(57) 【要約】 (修正有)

【課題】 コンピュータテストツールとクラウドベースサーバとの間の安全なデータ通信システムを提供する。

【解決手段】 システムは、コンピュータネットワーク上で診断テストを行うように構成されたコンピュータテストツール302を備える。システムは、コンピュータテストツール302からテストデータを受信し、それをキャッシュするとともに、通信ネットワーク308に無線で結合するために、コンピュータテストツール302と結合するように構成された通信デバイス306を更に備える。更にシステムは、通信デバイス306から送信されたテストデータを受信するように通信ネットワーク308に結合するように構成されたクラウドベースのサーバ304を備え、このテストデータがコンピュータテストツール302内で暗号化されるとともに、クラウドベースのサーバ304で復号化される。

【選択図】 図3



【特許請求の範囲】**【請求項 1】**

データ通信を提供するシステムであって、

コンピュータネットワーク上で1つ又は2つ以上の診断テストを行うとともに関連するテストデータを出力するように構成された少なくとも1つのコンピュータテストツールと

、
前記少なくとも1つのコンピュータテストツールから前記テストデータを受信してキャッシュするとともに、通信ネットワークに無線で結合するために、前記少なくとも1つのコンピュータテストツールと結合するように構成された少なくとも1つの通信デバイスと

、
前記少なくとも1つの通信デバイスから送信されたテストデータを受信するように前記通信ネットワークに結合するように構成されたクラウドベースのサーバと、を備え、

前記テストデータが前記少なくとも1つのコンピュータテストツールで暗号化されているとともに、前記クラウドベースのサーバで復号化されている、システム。

【請求項 2】

前記テストデータが前記少なくとも1つのコンピュータテストツールに関連付けられた秘密鍵を用いて暗号化されており、前記クラウドベースのサーバで前記少なくとも1つのコンピュータテストツールに関連付けられた公開鍵を用いて復号化されている、請求項1に記載のシステム。

【請求項 3】

前記クラウドベースのサーバが、前記通信ネットワーク及び前記少なくとも1つの通信デバイスを介して前記少なくとも1つのコンピュータテストツールで受信されるべき暗号化されたデータを送信するように更に構成されている、請求項1に記載のシステム。

【請求項 4】

前記少なくとも1つのコンピュータテストツールが、前記クラウドベースのサーバから送信された前記暗号化されたデータを復号化するように更に構成されている、請求項3に記載のシステム。

【請求項 5】

前記クラウドベースのサーバから送信された前記データが、前記クラウドベースのサーバに関連付けられた秘密鍵を用いて暗号化されており、前記少なくとも1つのコンピュータテストツールで前記クラウドベースのサーバに関連付けられた公開鍵を用いて復号化されている、請求項4に記載のシステム。

【請求項 6】

前記少なくとも1つのコンピュータテストツールが、前記少なくとも1つの通信デバイスとのデータ通信を確立するまで、1つ又は2つ以上の診断テストから生じるテストデータをキャッシュするように更に構成されている、請求項1に記載のシステム。

【請求項 7】

前記少なくとも1つのコンピュータテストツールが、Bluetooth（登録商標）、WiFi、USB結合、及びNFCのうち1つから選択される通信プロトコルから前記少なくとも1つの通信デバイスとのデータ通信を確立する、請求項6に記載のシステム。

【請求項 8】

前記少なくとも1つの通信デバイスが、前記少なくとも1つの通信デバイスと前記クラウドベースのサーバとの間で通信が確立されるまで、前記少なくとも1つのコンピュータテストツールから受信した暗号化されたテストデータをキャッシュするように更に構成されている、請求項1に記載のシステム。

【請求項 9】

前記少なくとも1つの通信デバイスが、スマートフォンデバイス及びタブレットデバイスからなるグループから選択されている、請求項1に記載のシステム。

【請求項 10】

前記コンピュータテストツールは、前記少なくとも1つの通信デバイスに、前記テスト

10

20

30

40

50

データの複数のコピーを送信し、それぞれのコピーは、関連するテストデータを識別する同一の識別タグに関連付けられており、

前記テストデータのコピーを受信することに対応して、前記クラウドベースのサーバは、前記識別されたテストデータの受信通知を前記コンピュータテストツールに送信し、

前記受信通知の受信に対応して、前記コンピュータテストツールはそれに関連付けられた前記識別タグを有する前記テストデータのすべてのコピーを削除する命令を有するメッセージを、前記少なくとも1つの通信デバイスに送信する、

請求項3に記載のシステム。

【請求項11】

前記クラウドベースのサーバは、前記少なくとも1つの通信デバイスに、制御又は構成データの複数のコピーを送信し、それぞれのコピーは、関連する制御又は構成データを識別する同一の識別タグに関連付けられており、

前記テストデータのコピーを受信することに対応して、前記コンピュータテストツールは、前記識別された制御又は構成データの受信通知を前記クラウドベースのサーバに送信し、

前記受信通知の受信に対応して、前記クラウドベースのサーバはそれに関連付けられた前記識別タグを有する前記制御又は構成データのすべてのコピーを削除する命令を有するメッセージを、前記少なくとも1つの通信デバイスに送信する、

請求項3に記載のシステム。

【請求項12】

前記少なくとも1つのコンピュータテストツール及び前記クラウドベースのサーバは、前記少なくとも1つの通信デバイスと交換される前記データを、前記少なくとも1つのコンピュータテストツール、前記少なくとも1つの通信デバイス、又は前記クラウドベースのサーバのうちいずれかによって記憶された前記診断データのいずれかのコピーが削除されるように指定された後の時間を示す関連する満了時間と関連付けるように更に構成されている、請求項1に記載のシステム。

【請求項13】

前記少なくとも1つのコンピュータテストツール、前記少なくとも1つの通信デバイス、及び前記クラウドベースのサーバが、現在時刻の後である関連する満了時間を有する記憶又は受信されたデータのいずれかのコピーを削除するように更に構成されている、請求項12に記載のシステム。

【請求項14】

テストデータを通信するためのコンピュータテストツールであって、

実行可能な命令を記憶するように構成されたメモリと、

前記メモリと通信して配置されたプロセッサと、を備え、前記プロセッサは、前記命令が実行されると、

コンピュータネットワーク上で1つ又は2つ以上の診断テストを行うとともに関連するテストデータを出力し、

前記テストデータをキャッシュし、

前記テストデータを暗号化し、

前記暗号化されたテストデータを通信デバイスに送信するように構成されており、前記送信された暗号化されたテストデータは、前記通信デバイスと結合されたクラウドベースのサーバにより復号化されるように構成されている、コンピュータテストツール。

【請求項15】

前記コンピュータテストツールは、暗号化されたデータを前記クラウドベースのサーバから前記通信ネットワーク及び前記少なくとも1つの通信デバイスを介して受信する、請求項14に記載のコンピュータテストツールシステム。

【請求項16】

前記コンピュータテストツールは、前記クラウドベースのサーバから受信した前記暗号化されたデータを復号化するように更に構成されている、請求項15に記載のコンピュー

10

20

30

40

50

タテストツール。

【請求項 17】

前記クラウドベースのサーバから受信した前記データは、前記クラウドベースのサーバに関連付けられた秘密鍵を用いて暗号化されており、前記コンピュータテストツールで前記クラウドベースのサーバに関連付けられた公開鍵を用いて復号化されている、請求項 16 に記載のコンピュータテストツール。

【請求項 18】

前記コンピュータテストツールは、前記コンピュータテストツールが前記少なくとも 1 つの通信デバイスとのデータ通信を確立するまで、前記テストデータをキャッシュする、請求項 14 に記載のコンピュータテストツール。

10

【請求項 19】

データ通信を提供するためのクラウドベースのサーバであって、

実行可能な命令を記憶するように構成されたメモリと、

前記メモリと通信して配置されたプロセッサと、を備え、前記プロセッサは、前記命令の実行により、

通信ネットワークを介した通信デバイスと前記クラウドベースのサーバとの通信が確立されると、暗号化されたテストデータを通信デバイスから受信し、前記テストデータがコンピュータテストデバイスで行われる診断テスト中に取得され、前記コンピュータテストデバイスでキャッシュ及び暗号化され、前記クラウドベースのサーバで復号化され、前記通信デバイスと前記コンピュータテストデバイスとの間の通信が確立されると、前記通信デバイスに送信されるように構成され、

20

前記暗号化されたテストデータを復号化する、ように構成されている、クラウドベースのサーバ。

【発明の詳細な説明】

【技術分野】

【0001】

開示された実施形態は一般に、テスト装備モニタリング用のシステム及び方法に関し、特に、コンピュータテストツールとクラウドベースのサーバとの間の安全なシステム及び方法に関する。

【0002】

テスト装備、例えば、コンピュータテストツールは、クラウドベースの（クラウドベースとも呼ばれる）サーバと通信することができる場合がある。いくつかの構成では、コンピュータテストツール及びサーバは両方とも、データを交換するために同時にネットワークに結合されなければならない。しかし、コンピュータテストツールは、データ交換が必要とされる重大なときにデータを交換するためのネットワーク接続にアクセスできない場合がある。

30

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】米国特許出願公開番号 2015/0006894

40

【発明の概要】

【発明が解決しようとする課題】

【0004】

ネットワークへのアクセスを提供するために、スマートフォン、タブレット、又はラップトップなどのモバイルデバイスは、コンピュータテストツールに結合され、コンピュータテストツールからデータを収集し、記憶するとともに、後にそのデータをサーバに送信することができる。しかし、侵入者は、コンピュータテストツール又は通信デバイスになりすまして、偽物又は偽造の診断データをサーバに送信することができる。別のシナリオでは、侵入者は、サーバ又は通信デバイスになりすまして、偽物又は偽造の制御又は構成データをコンピュータテストツールに送信することができる。

50

【課題を解決するための手段】

【0005】

後述する例示の実施形態の目的及び利点は、以下の説明に説明され、それから明らかであろう。例示の実施形態の更なる利点は、記載された説明及び特許請求の範囲、並びに添付の図面において特に記載されるデバイス、システム及び方法によって実現及び達成されるであろう。

【0006】

これら及び他の利点を達成するために、例示の実施形態の目的に従って、一態様では、データ通信を提供するシステムが記載される。本システムは、コンピュータネットワーク上で1つ又は2つ以上の診断テストを行うように構成された少なくとも1つのコンピュータテストツールを備える。本システムは、少なくとも1つのコンピュータテストツールから前記テストデータを受信してキャッシュするとともに、通信ネットワークに無線で結合するために、少なくとも1つのコンピュータテストツールと結合するように構成された少なくとも1つの通信デバイスを更に備える。加えて、本システムは、少なくとも1つの通信デバイスから送信されたテストデータを受信するように通信ネットワークに結合するように構成されたクラウドベースのサーバと、を備え、前記テストデータが少なくとも1つのコンピュータテストツールで暗号化されているとともに、クラウドベースのサーバで復号化されている。

10

【0007】

実施形態では、テストデータが少なくとも1つのコンピュータテストツールに関連付けられた秘密鍵を用いて暗号化されており、クラウドベースのサーバで少なくとも1つのコンピュータテストツールに関連付けられた公開鍵を用いて復号化され得る。クラウドベースのサーバが、通信ネットワーク及び少なくとも1つの通信デバイスを介して少なくとも1つのコンピュータテストツールで受信されるべき暗号化されたデータを送信するように更に構成され得る。

20

【0008】

更にまた、実施形態では、少なくとも1つのコンピュータテストツールが、クラウドベースのサーバから送信された暗号化されたデータを復号化するように更に構成されている。クラウドベースのサーバから送信されたデータが、クラウドベースのサーバに関連付けられた秘密鍵を用いて暗号化され得、少なくとも1つのコンピュータテストツールでクラウドベースのサーバに関連付けられた公開鍵を用いて復号化されている。少なくとも1つのコンピュータテストツールが、少なくとも1つのコンピュータテストツールが少なくとも1つの通信デバイスとのデータ通信を確立するまで、1つ又は2つ以上の診断テストから生じるテストデータをキャッシュするように更に構成され得る。少なくとも1つのコンピュータテストツールが、Bluetooth（登録商標）、WiFi、USB結合、及びNFCのうち1つから選択される通信プロトコルから少なくとも1つの通信デバイスとのデータ通信を確立することができる。

30

【0009】

更に、実施形態では、少なくとも1つの通信デバイスが、少なくとも1つの通信デバイスとクラウドベースのサーバとの間で通信が確立されるまで、少なくとも1つのコンピュータテストツールから受信した暗号化されたテストデータをキャッシュするように更に構成され得る。少なくとも1つの通信デバイスが、スマートフォンデバイス及びタブレットデバイスからなるグループから選択され得る。

40

【0010】

実施形態では、コンピュータテストツールは、少なくとも1つの通信デバイスに、テストデータの複数のコピーを送信し、それぞれのコピーは、関連するテストデータを識別する同一の識別タグに関連付けられている。テストデータのコピーを受信することに応答して、クラウドベースのサーバは、識別されたテストデータの受信通知をコンピュータテストツールに送信することができる。受信通知の受信に応答して、前記コンピュータテストツールはそれに関連付けられた前記識別タグを有する前記テストデータのすべてのコピー

50

を削除する命令を有するメッセージを、前記少なくとも1つの通信デバイスに送信することができる。

【0011】

また、実施形態では、クラウドベースのサーバは、少なくとも1つの通信デバイスに、制御又は構成データの複数のコピーを送信ことができ、それぞれのコピーは、関連する制御又は構成データを識別する同一の識別タグに関連付けられている。テストデータのコピーを受信することに対応して、コンピュータテストツールは、識別された制御又は構成データの受信通知をクラウドベースのサーバに送信することができる。受信通知の受信に対応して、クラウドベースのサーバはそれに関連付けられた識別タグを有する制御又は構成データのすべてのコピーを削除する命令を有するメッセージを、前記少なくとも1つ

10

【0012】

加えて、実施形態では、少なくとも1つのコンピュータテストツール及びクラウドベースのサーバは、少なくとも1つの通信デバイスと交換されるデータを、少なくとも1つのコンピュータテストツール、少なくとも1つの通信デバイス、又はクラウドベースのサーバのうちいずれかによって記憶された診断データのいずれかのコピーが削除されるように指定された後の時間を示す関連する満了時間と関連付けるように更に構成され得る。少なくとも1つのコンピュータテストツール、少なくとも1つの通信デバイス、及びクラウドベースのサーバが、現在時刻より遅い関連する満了時間を有する記憶又は受信されたデータのいずれかのコピーを削除するように更に構成され得る。

20

【0013】

更なる任意の態様では、テストデータを通信するためのコンピュータテストツールが記載されている。コンピュータテストツールは、実行可能な命令を記憶するように構成されたメモリと、メモリと通信して配置されたプロセッサと、を備え、プロセッサは、命令が実行されると、コンピュータネットワーク上で1つ又は2つ以上の診断テストを行うとともに関連するテストデータを出力し、このテストデータをキャッシュし、このテストデータを暗号化し、暗号化されたテストデータを通信デバイスに送信するように構成されており、送信された暗号化されたテストデータは、通信デバイスと結合されたクラウドベースのサーバにより復号化されるように構成されている。

【0014】

実施形態では、コンピュータテストツールは、暗号化されたデータをクラウドベースのサーバから通信ネットワーク及び少なくとも1つの通信デバイスを介して受信することができる。コンピュータテストツールは、クラウドベースのサーバから受信した暗号化されたデータを復号化するように更に構成され得る。クラウドベースのサーバから受信されたデータは、クラウドベースのサーバに関連付けられた秘密鍵を用いて暗号化され得、コンピュータテストツールでクラウドベースのサーバに関連付けられた公開鍵を用いて復号化され得る。コンピュータテストツールは、このコンピュータテストツールが少なくとも1つの通信デバイスとのデータ通信を確立するまで、テストデータをキャッシュすることができる。

30

【0015】

追加の任意の態様では、データ通信を提供するためのクラウドベースのサーバが記載されている。クラウドベースのサーバは、実行可能な命令を記憶するように構成されたメモリと、メモリと通信して配置されたプロセッサと、を備え、プロセッサは、命令の実行により、通信ネットワークを介した通信デバイスとクラウドベースのサーバとの通信が確立されると、暗号化されたテストデータを通信デバイスから受信するように構成され、テストデータがコンピュータテストデバイスで行われる診断テスト中に取得され、コンピュータテストデバイスでキャッシュ及び暗号化され、クラウドベースのサーバで復号化され、通信デバイスとコンピュータテストデバイスとの間の通信が確立されると、通信デバイスに送信されるように構成されている。プロセッサは、命令の実行により、暗号化されたテストデータを復号化するように更に構成されている。

40

50

【図面の簡単な説明】

【0016】

添付の付属書類及び／又は図面は、本開示による様々な非限定的な例示の、発明的側面を例証する。

【図1】図1は、例示的な通信ネットワークを図示する。

【図2】図2は、例示的なネットワークデバイス／ノードを図示する。

【図3】図3は、本開示によるクラウド支援診断システムを例証するフローチャートである。

【図4】図4は、本開示による安全に診断データを送信するためにコンピュータテストツールによって行われる方法を例証するフローチャートである。

【図5】図5は、本開示による安全に制御及び構成データを受信するためにコンピュータテストツールによって行われる方法を例証するフローチャートである。

【図6】図6は、本開示によるコンピュータテストツール又はサーバと安全にデータを交換するために通信デバイスによって行われる方法を例証するフローチャートである。

【図7】図7は、本開示による安全に診断データを受信するためにサーバによって行われる方法を例証するフローチャートである。

【図8】図8は、本開示による安全に制御及び構成データを送信するためにサーバによって行われる方法を例証するフローチャートである。

【図9】図9は、本開示による複数の通信デバイスを有するクラウド支援診断システムを例証するフローチャートである。

【発明を実施するための形態】

【0017】

ここで、同様の参照数字が同様の構造的／機能的特徴を特定する添付図面を参照して、例示の実施形態を更に十分に説明する。例示の実施形態は、いかなる方法でも図示されたものに限定されるものではなく、後述する例示の実施形態は、当業者には明らかなように、種々の形態で具現化され得る単なる典型例にすぎない。したがって、本明細書に開示されるいかなる構造的かつ機能的な詳細も限定としてではなく、単に特許請求の範囲についての基礎として、また、当業者に検討される実施形態を様々に用いるよう教示するための代表例として解釈すべきであることが理解されよう。更に、本明細書で使用される語句は、限定のためのものではなく、例示の実施形態を理解可能に説明するためのものである。

【0018】

特に規定のない限り、本明細書で使用されるすべての技術用語及び科学用語は、本発明が属する分野の当業者に一般的に理解されるのと同じ意味を有する。本明細書において説明するものと同様又は等価な任意の方法及び材料を、例示の実施形態を実施又は試験する際に使用することができるが、典型的な方法を以下に説明する。

【0019】

本明細書及び添付の特許請求の範囲において使用するとき、単数形「a」、「an」、及び「the」は、その内容について別段の明確な指示がない限り、複数の指示対象を含むことに留意しなければならない。したがって、例えば、「刺激」への言及は、複数のかかる刺激を含み、「信号」と言及した場合は、1つ若しくは2つ以上の信号及び当業者に知られたその同等物などへの言及を含む。

【0020】

以下で検討する例示の実施形態は、好ましくは、コンピュータプロセッサを有するマシン上での実行を可能にするための制御論理を有するコンピュータ使用可能媒体上に置かれたソフトウェアアルゴリズム、プログラム又はコードとすることができることを理解すべきである。マシンは、典型的には、コンピュータアルゴリズム又はプログラムの実行からの出力を提供するように構成されたメモリ記憶装置を含む。

【0021】

本明細書に使用するとき、「ソフトウェア」という用語は、その実装がハードウェア、ファームウェアの中、又はディスク上で利用可能なソフトウェアコンピュータ製品、メモ

10

20

30

40

50

リ記憶デバイスとして、若しくは、リモートマシンからのダウンロード用であるかにかかわらず、ホストコンピュータのプロセッサの中にある、任意のコード又はプログラムと同義であることを意味する。本明細書に記載する実施形態は、上述した式、関係、アルゴリズムを実装するかかるソフトウェアを含む。当業者であれば、上述した実施形態に基づいて例示の実施形態の更なる特徴及び利点を理解するであろう。したがって、例示の実施形態は、添付の特許請求の範囲に示されるもの以外には、具体的に示し、記載してきたものに限定されない。

【0022】

ここで記述するために図面に戻ると、同様の参照符号は、複数の図面を通じて同様の要素を表しており、図1は、以下の例示の実施形態が実装され得る典型的な通信ネットワーク100を示す。

10

【0023】

通信ネットワーク100は、通信リンクによって相互に接続されたノードと、パーソナルコンピュータ、ワークステーション、スマートフォンデバイス、タブレット、テレビジョン、センサ及び又は自動車などの他のデバイスなどのエンドノード間でデータを伝送するためのセグメントとの地理的に分散された集合であることを理解すべきである。ローカルエリアネットワーク(LAN)からワイドエリアネットワーク(WAN)の範囲の多くの種類のネットワークが利用可能である。典型的には、LANは、建物又はキャンパスなどの同じ大まかな物理的場所に置かれた専用の私設通信リンクを介してノードを接続する。一方、WANは、典型的には、よくある回線事業者の加入電話回線、光学的光経路、同期光ネットワーク(SONET)、同期デジタルハイアラキ(SDH)リンク、電力線通信(PLC)などの長距離通信リンクを介して地理的に分散したノードを接続する。

20

【0024】

図1は、様々な通信方法によってリンク109を介して相互に接続されたノード/デバイス101~108(例えば、センサ102、クライアントコンピューティングデバイス103、スマートフォンデバイス105、Webサーバ106、ルータ107、スイッチ108など)を例示として含む例示的な通信ネットワーク100の概略ブロック図である。例えば、リンク109は、有線リンクであってもよく、又は、例えば、距離、信号強度、現在の動作状態、位置などに基づいて、特定のノードが他のノードと通信する無線通信媒体を含んでもよい。また、デバイスのそれぞれは、必要な場合、様々な有線プロトコル及び無線プロトコルなどの、当業者により理解される事前に定義されたネットワーク通信プロトコルを用いてデータパケット(又はフレーム)142を他のデバイスと通信することができる。この状況において、プロトコルは、ノードが互いにどのように相互作用するかを規定する1組の規則からなる。当業者であれば、任意の数のノード、デバイス、リンクなどがコンピュータネットワークに用いられ得ること、更に本明細書に示す図面は簡略化のためであることを理解するであろう。また、実施形態は一般のネットワーククラウドを参照して本明細書に示されるが、本明細書の記載はそのように限定されるものではなく、ハードウェアにより実現されるネットワークに適用され得る。

30

【0025】

当業者によって理解されるように、本発明の態様は、システム、方法又はコンピュータプログラム製品として具現化され得る。したがって、本発明の態様は、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)又は、本明細書において一般的にすべて「回路」、「モジュール」、又は「システム」と呼ばれ得るソフトウェア態様とハードウェア態様とを組み合わせた実施形態をとることができる。更に、本発明の態様は、コンピュータ読み取り可能なプログラムコードが組み込まれた1つ又は2つ以上のコンピュータ読み取り可能な媒体に組み込まれたコンピュータプログラム製品の形態をとることができる。

40

【0026】

1つ又は2つ以上のコンピュータ読み取り可能な媒体の任意の組み合わせを利用してよい。コンピュータ読み取り可能な媒体はコンピュータ読み取り可能な信号媒体であって

50

も、コンピュータ読み取り可能な記憶媒体であってもよい。コンピュータ読み取り可能な記憶媒体は、例えば、電氣的、磁氣的、光學的、電磁氣的、赤外線、若しくは半導体システム、装置、若しくはデバイス、又は前述の任意の好適な組み合わせとすることができるが、これらに限定されない。コンピュータ読み取り可能な記憶媒体のより具体的な例（非限定的リスト）としては、以下のもの、即ち、1つ又は2つ以上のワイヤを有する電氣的接続、ポータブルコンピュータディスク、ハードディスク、ランダムアクセスメモリ（RAM）、リードオンリメモリ（ROM）、消去可能なプログラマブル読み取り専用メモリ（EPROM又はフラッシュメモリ）、光ファイバ、ポータブルコンパクトディスク読み取り専用メモリ（CD-ROM）、光記憶デバイス、磁気記憶デバイス、又は前述の任意の好適な組み合わせが挙げられるであろう。本明細書の文脈においては、コンピュータ読み取り可能な記憶媒体は、命令実行システム、装置、若しくはデバイスによって使用される、又はそれらと関連して使用されるプログラムを包含又は記憶することができる任意の有形媒体とすることができる。

10

20

30

40

50

【0027】

コンピュータ読み取り可能な信号媒体は、伝播データ信号と、その中、例えば、ベースバンド、又は搬送波の一部として組み込まれたコンピュータ読み取り可能なプログラムコードを含む場合がある。かかる伝播信号は、電磁氣的、光學的、又はこれらの任意の好適な組み合わせを含む様々な形態のいずれかをとることができるが、これらに限定されない。コンピュータ読み取り可能な信号媒体は、コンピュータ読み取り可能な記憶媒体ではなく、命令実行システム、装置、若しくはデバイスによって使用される、又はこれらと関連して使用されるプログラムを通信、伝播、又は伝送できる任意のコンピュータ読み取り可能な媒体とすることができる。

【0028】

コンピュータ読み取り可能な媒体に組み込まれたプログラムコードは、限定されるものではないが、無線、有線、光ファイバケーブル、RFなど、又は前述の任意の好適な組み合わせを含む任意の適切な媒体を用いて送信され得る。

【0029】

本発明の態様のオペレーションを実行するためのコンピュータプログラムコードは、Java（登録商標）、Smalltalk、C++などのオブジェクト指向プログラミング言語及び「C」プログラミング言語又は同様のプログラミング言語などの従来の手続き型プログラミング言語を含む、1つ又は2つ以上のプログラミング言語の任意の組み合わせで書かれる場合がある。プログラムコードは、ユーザのコンピュータ上で完全に、ユーザのコンピュータ上で部分的に、部分的にユーザのコンピュータ上でかつ部分的にリモートコンピュータ上でスタンドアロンソフトウェアパッケージとして、又は完全にリモートコンピュータ若しくはサーバ上で実行する場合がある。後半のシナリオでは、リモートコンピュータは、ローカルエリアネットワーク（LAN）又はワイドエリアネットワーク（WAN）を含む任意の種類のネットワークを通してユーザのコンピュータに接続される場合があり、あるいは、その接続は、外部コンピュータ（例えば、インターネットサービスプロバイダーを用いてインターネットを通して）に対して行われ得る。

【0030】

本発明の態様を、本発明の実施形態にかかる方法、装置（システム）及びコンピュータプログラム製品のフローチャート図及び/又はブロック図を参照して以下に説明する。フローチャート図及び/又はブロック図の各ブロック、並びにフローチャート図及び/又はブロック図の中のブロックの組み合わせは、コンピュータプログラム命令によって実装され得ることが理解されるであろう。これらのコンピュータプログラム命令は、汎用コンピュータ、専用コンピュータ、又はマシンを生成するための他のプログラマブルデータ処理装置のプロセッサに提供される場合があり、コンピュータ又は他のプログラマブルデータ処理装置のプロセッサを介して実行する命令は、フローチャート及び/又はブロック図のブロック若しくは複数のブロックに指定された機能/動作を実装するための手段を作成する。

【0031】

これらのコンピュータプログラム命令はまた、コンピュータ、他のプログラマブルデータ処理装置、又は他のデバイスに特定の方法で機能するように指示することができるコンピュータ読み取り可能な媒体に記憶される場合もあり、コンピュータ読み取り可能な媒体に記憶されたこの命令により、フローチャート及び/又はブロック図のブロック若しくは複数のブロックに指定された機能/行動を実装する命令を含む製品が製造される。

【0032】

コンピュータプログラム命令はまた、コンピュータ、他のプログラマブルデータ処理装置、又は他のデバイスにロードされ、コンピュータ実装プロセスを生成するように一連の動作工程がコンピュータ、他のプログラマブル装置、又は他のデバイス上で実行される場合もあり、コンピュータ又は他のプログラマブル装置上で実行する命令は、フローチャート及び/又はブロック図のブロック若しくは複数のブロックに指定された機能/動作を実装するためのプロセスを提供する。

10

【0033】

図2は、例えば、ネットワーク100に示すノードの1つとして、本明細書に記載する1つ又は2つ以上の実施形態(又はそのコンポーネント)とともに使用され得る例示的なネットワークコンピューティングデバイス200(例えば、クライアントコンピューティングデバイス103、サーバ106など)の概略ブロック図である。上述したように、異なる実施形態では、これらの様々なデバイスは、例えば、通信ネットワーク100を介して任意の好適な方法で互いに通信するように構成されている。

20

【0034】

デバイス200は、本発明の様々な実施形態の教示を実行できる任意の種類のコピュータシステムを表すように意図されている。デバイス200は好適なシステムの単なる一例にすぎず、本明細書に記載する発明の実施形態の用途又は機能性の範囲に関するいかなる限定を提示するように意図されるものではない。にもかかわらず、コンピューティングデバイス200は、本明細書で説明した機能性のいずれかを実装され得る及び/又は実行し得る。

【0035】

コンピューティングデバイス200は、多数の他の汎用若しくは専用コンピューティングシステム環境又は構成で動作する。コンピューティングデバイス200で使用するのに好適であり得る周知のコンピューティングシステム、環境、及び/又は構成の実施例としては、パーソナルコンピュータシステム、サーバコンピュータシステム、シンクライアント、シッククライアント、ハンドヘルド又はラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースのシステム、セットトップボックス、プログラマブル家電、ネットワークPC、ミニコンピュータシステム、及び上記システム又はデバイスなどのいずれかを含む分散データ処理環境が挙げられるが、これらに限定されない。

30

【0036】

コンピューティングデバイス200は、コンピュータシステムによって実行されるプログラムモジュールなどのコンピュータシステム実行可能命令の一般的な文脈において説明されてもよい。一般に、プログラムモジュールは、ルーチン、プログラム、オブジェクト、コンポーネント、ロジック、データ構造などを含んでもよく、これらは、特定のタスクを実行し、又は特定の抽象データ型を実装する。コンピューティングデバイス200は、タスクが通信ネットワークを通してリンクされるリモート処理デバイスによって行われる分散データ処理環境で実施され得る。分散データ処理環境では、プログラムモジュールは、メモリ記憶デバイスを含むローカル及びリモートコンピュータシステム記憶媒体の両方に置かれてもよい。

40

【0037】

デバイス200を、汎用コンピューティングデバイスの形態で図2に示す。デバイス200のコンポーネントは、1つ又は2つ以上のプロセッサ又は処理装置216、システムメモリ228、及び、システムメモリ228を含む様々なシステムコンポーネントをプロ

50

セッサ 216 に結合するバス 218 を含むことができるが、これらに限定されない。

【0038】

バス 218 は、メモリバス又はメモリコントローラ、周辺バス、アクセラレーテッドグラフィックスポート、及び様々なバスアーキテクチャのうちいずれかを用いたプロセッサ又はローカルバスを含む、いくつかの種類のバス構造のいずれかのうち1つ又は2つ以上を表す。一例として、かかるアーキテクチャとしては、インダストリスタンダードアーキテクチャ (ISA) バス、マイクロチャンネルアーキテクチャ (MCA) バス、拡張 ISA (EISA) バス、ビデオエレクトロニクススタンダードアソシエーション (VESA) ローカルバス、及び周辺コンポーネント相互接続 (PCI) バスが挙げられるが、これらに限定されない。

10

【0039】

コンピューティングデバイス 200 は、典型的には、様々なコンピュータシステム読み取り可能な媒体を含む。かかる媒体は、デバイス 200 によってアクセス可能な任意の利用可能な媒体とすることができ、それは、揮発性及び不揮発性媒体、リムーバブル媒体及び非リムーバブル媒体の両方を含む。

【0040】

システムメモリ 228 は、ランダムアクセスメモリ (RAM) 230 及び / 又はキャッシュメモリ 232 などの揮発性メモリの形態のコンピュータシステム読み取り可能な媒体を含むことができる。コンピューティングデバイス 200 は、他のリムーバブル / 非リムーバブル、揮発性 / 不揮発性コンピュータシステム記憶媒体を更に含むことができる。ほんの一例として、記憶システム 234 は、非リムーバブル、不揮発性磁気媒体 (図示されていない、典型的には「ハードディスク」と呼ばれる) から読み出す、かつそれに書き込むために提供され得る。図示しないが、リムーバブル、不揮発性磁気ディスク (例えば、「フロッピーディスク」) から読み取り、またそれに書き込むための磁気ディスクドライブ、及び、CD-ROM、DVD-ROM 又は他の光媒体などのリムーバブル、不揮発性光ディスクから読み取り、またそれに書き込むための光ディスクドライブが提供され得る。そのような場合、それぞれは、1つ又は2つ以上のデータ媒体インタフェースによってバス 218 に接続され得る。下記に更に図示し説明するように、メモリ 228 は、本発明の実施形態の機能を実行するように構成されている 1 組 (例えば、少なくとも 1 つ) のプログラムモジュールを有する少なくとも 1 つのプログラム製品を含むことができる。

20

30

【0041】

アンダーライティングモジュールなどの 1 組 (少なくとも 1 つ) のプログラムモジュール 215 を有するプログラム / ユーティリティ 240 は、一例として、限定するものではなく、メモリ 228 に、オペレーティングシステム、1つ又は2つ以上のアプリケーションプログラム、他のプログラムモジュール、及びプログラムデータと同様に、記憶され得る。オペレーティングシステム、1つ又は2つ以上のアプリケーションプログラム、他のプログラムモジュール、及びプログラムデータのそれぞれ、あるいはそれらの一部の組み合わせは、ネットワーク環境の実装を含む場合がある。プログラムモジュール 215 は一般に、本明細書に記載する本発明の実施形態の機能及び / 又は方法を実行する。

【0042】

デバイス 200 はまた、キーボード、ポインティングデバイス、ディスプレイ 224 などの 1つ又は2つ以上の外部デバイス 214、ユーザにコンピューティングデバイス 200 と相互作用することを可能にする 1つ又は2つ以上のデバイス、及び / 又はコンピューティングデバイス 200 に 1つ又は2つ以上の他のコンピューティングデバイスと通信するのを可能にする任意のデバイス (例えば、ネットワークカード、モデムなど) と通信することもできる。そのような通信は、入力 / 出力 (I/O) インタフェース 222 を介して発生することができる。更にまた、デバイス 200 は、ローカルエリアネットワーク (LAN)、一般のワイドエリアネットワーク (WAN)、及び / 又は公共ネットワーク (例えば、インターネット) などの 1つ又は2つ以上のネットワークとネットワークアダプタ 220 を介して通信することができる。図示するように、ネットワークアダプタ 220

40

50

は、コンピューティングデバイス200の他のコンポーネントとバス218を介して通信する。図示していないが、他のハードディスクコンポーネント及び/又はソフトウェアコンポーネントがデバイス200と組み合わせて使用され得ることを理解されたい。例として、マイクロコード、デバイスドライバ、冗長処理装置、外部ディスクドライブアレイ、RAIDシステム、テープドライブ、及びデータアーカイバル記憶システムなどが挙げられるが、これらに限定されない。

【0043】

以下の記述では、特定の実施形態を、図2のコンピューティングシステム環境200などの、1つ又は2つ以上のコンピューティングデバイスによって行われる動作(act)及びオペレーションの象徴的表現を参照して説明することができる。ゆえに、しばしばコンピュータに実行されるものとして参照されるかかる動作及びオペレーションは、構造化された形態のデータを表す電気信号のコンピュータプロセッサによる操作を含むことが理解されるであろう。この操作は、データを変換し、又はコンピュータのメモリシステムの場所で保持し、コンピュータのオペレーションを、当業者が理解する方法で再構成するか、さもなければ、変更する。データが保持されるデータ構造は、データのフォーマットにより規定される特定の性質を有するメモリの物理的場所である。しかし、実施形態は前述の文脈で説明されているが、限定を意味するものではなく、後述する動作及びオペレーションがまたハードウェアに実装され得ることを当業者が理解するであろう。

【0044】

図1及び図2は、後述する本発明の実施形態が実装され得る説明的かつ/又は好適な典型的環境の簡潔で一般的な記述を提供することを意図するものである。図1及び図2は好適な環境の典型であり、本発明の実施形態の構造、用途の範囲、又は機能性に関するいかなる限定を提示することを意図するものではない。特定の環境は、典型的な動作環境に説明されるコンポーネントのいずれか1つ又は組み合わせに関する任意の依存性又は要求性を有するものとして解釈されるべきではない。例えば、特定の場合には、環境の1つ又は2つ以上の要素は必要ではなく、省略されてもよい。他の場合には、1つ又は2つ以上の他の要素は、必要であり、追加されてもよい。

【0045】

典型的な通信ネットワーク100(図1)及びコンピューティングデバイス200(図2)を一般的に示し上記で検討してきたが、ここで本発明の特定の例示の実施形態について記述する。ここで図3~図5を参照して、クラウド支援診断システム300を一般的に示す。ここで、コンピュータテストツール302がクラウドベースのサーバ304と通信デバイス306を介して間接的に通信し、コンピュータテストツール302とサーバ304との間の通信が確保され、通信デバイス304が通信のコンテンツにアクセスするのを防止し、更に偽造メッセージがコンピュータテストツール302及び/又はサーバ304に送信されるのを防止する。

【0046】

コンピュータテストツール302及び通信デバイス306は、それぞれ、図1に示す通信ネットワーク100と同様に構成され得る第1のネットワークのノード(例えば、ノード101~105、107、又は108)として機能する各コンピュータシステムとすることができる。コンピュータテストツール302及び通信デバイス306は、少なくとも1つの第1の通信リンク308を介して互いに通信する。同様に、サーバ304は、ノード(例えば、ノード106)として機能するコンピュータシステムであり、通信デバイス306は、通信ネットワーク100と同様に構成され得る第2のネットワーク308のノード(例えば、ノード101~105、107、又は108)として機能する。

【0047】

このように、公開鍵の暗号化は非対称鍵アルゴリズムを使用し、暗号化又は復号化のいずれかを行うために一方のデバイスにより用いられる鍵は、対応するオペレーションにおいて他方のデバイスにより用いられる鍵と同一ではない。公開鍵の暗号化を用いた双方向通信に係る各デバイスは、一对の暗号鍵(公開暗号化鍵及び秘密復号化鍵)を備えて

10

20

30

40

50

いる。公開鍵は、広く分布され得るが、秘密鍵はその所有者だけが知っている。鍵は、数学的に関連するが、パラメータは、秘密鍵を公開鍵から計算することが実行不可能なように選ばれる。

【0048】

コンピュータテストツール302、通信デバイス306、及びサーバ304は、それぞれ、処理装置216、ネットワークアダプタ220、I/Oインタフェース222、及びメモリ228を含むためなど、図2に示すネットワークコンピューティングデバイス200と同様に構成され得る。第1、第2、及び第3の通信リンク310、312、314は、それぞれ単一又は複数の有線及び/又は無線リンクを含むことができる。実施形態では、これらのリンクの一部は、無線周波数認識(RFID)、Bluetooth(登録商標)、赤外線通信などの近距離無線通信を使用する。実施形態では、第2のネットワーク308はインターネットを含む。

10

【0049】

コンピュータテストツール302は、信号又は電源の電気特性、温度、作用する力など物理的実体の特性を測定するための1つ又は2つ以上のセンサを含む診断デバイス316を含むモバイル又は固定デバイスとすることができる。診断デバイス316は、必要に応じてアナログ・デジタル(A/D)変換と組み合わせて、測定に関連する少なくとも1つの値を示す診断データを出力する。

【0050】

診断デバイス302により出力された診断データは、メモリ228などの記憶デバイスに記憶される。例えば、出力診断データは、通信デバイス306に提出される前に、(例えば、キャッシュ232又は記憶システム234に)キャッシュ又は記憶され得る。加えて、コンピュータテストツール302は、(例えば、メモリ228に)コンピュータテストツール302によって、例えば、クライアント306に送信された診断データを暗号化するためのコンピュータテストツール(CTT)秘密鍵318を記憶する。コンピュータテストツール302は、サーバ304から受信したメッセージを復号化するためのサーバ304サーバに関連付けられた(S)公開鍵320を更に記憶する。CTT秘密鍵318及びS公開鍵320については以下でより詳細に検討する。

20

【0051】

要求により、かつ/又は通信リンク310の確立により、コンピュータテストツール302は、(例えば、ネットワークアダプタ220を介して)診断データを、通信リンク310を介してコンピュータテストツール302に結合された通信デバイス306に送信することができる。

30

【0052】

コンピュータテストツール302は、受信したメッセージがサーバ304から送信されること、また、サーバ304に送信されたメッセージがコンピュータテストツール302によって送信されたことを認証するために、通信デバイス306と交換された(例えば、それから受信した、又はそれに送信した)メッセージを処理する認証モジュール322(例えば、サーバ304のメモリ228によって記憶されたプログラムモジュール215)を含む。

40

【0053】

通信デバイス306は、コンピュータテストツール302とサーバ304との間でメッセージの交換を促進する媒介として機能する固定又はポータブルデバイス(例えば、電話、タブレット、又はラップトップ)とすることができる。一実施形態では、通信デバイス306は、WiFiサービスをコンピュータテストツール302に提供するホットスポットとして機能することができ、それによって、コンピュータテストツール302がWiFiを介してサーバ304と通信できるようになる。この実施形態では、コンピュータテストツール302に送信された、又はそれから送信されたデータは、通信デバイス306によってあて先に向けてルーティングされる。この実施形態における通信デバイス306は、ホットスポットとして機能できるようにするハードウェア及び/又はソフトウェア(例

50

えば、プログラムモジュール 2 1 5) を含む。

【 0 0 5 4 】

別の実施形態では、コンピュータテストツール 3 0 2 は、通信デバイス 3 0 6 にテザーされており、通信リンク 3 1 0 は、例えば、ケーブル（例えば、USB 若しくはイーサネット（登録商標））又はワイヤレス近距離無線通信を含むテザーされたリンクである。通信デバイス 3 0 6 は、通信リンク 3 1 0 を介したコンピュータテストツール 3 0 2 とのデータの交換、並びに通信 3 1 2 及びインターネットを介したサーバ 3 0 4 とのデータの交換を含む、コンピュータテストツール 3 0 2 とサーバ 3 2 4 との間の媒介として作用する。この実施形態の通信デバイス 3 0 6 は、通信リンク 3 1 0 が動作しているとき、コンピュータテストツール 3 0 2 から診断データを受信して、記憶するとともに、通信リンク 3 1 2 が動作しているとき、記憶された診断データをサーバ 3 0 4 に送信できるようにするハードウェア及び/又はソフトウェア（例えば、プログラムモジュール 2 1 5 ）を含む。一実施形態では、通信リンク 3 1 0 及び 3 1 2 の両方が動作しているとき、通信デバイス 3 0 6 は、診断データの記憶を差し控えることができる。

10

【 0 0 5 5 】

サーバ 3 0 4 は、（例えば、ネットワークアダプタ 2 2 0 を介して）第 2 のネットワーク 3 0 8 に通信リンク 3 1 4 を介して結合することによって 1 つ又は 2 つ以上の通信デバイス 3 0 6 と通信する web サーバである。有線、無線、又はそれらの組み合わせとすることができる通信リンク 3 1 4 は、動作時間中、通信デバイス 3 0 6 のうち 1 つと通信するために安定して容易に利用可能である。加えて、サーバ 3 0 4 は、通信デバイス 3 0 6 と通信するのに容易に利用可能であり、診断データを受信、処理、及び又は記憶するとともに、メッセージ、例えば、制御又は構成（c o r c）メッセージをコンピュータテストツール 3 0 2 に送信する。オペレーション時間は、例えば、1 日若しくは 1 週間のうちの指定された時間、又は動作不良若しくは定期保守がある時間以外の 1 日若しくは 1 週間（2 4 / 7）のうち任意の時間を含むことができる。

20

【 0 0 5 6 】

サーバ 3 0 4 は、（例えば、メモリ 2 2 8 に）サーバ 3 0 4 によって、例えば、クライアント 3 0 6 に送信された診断データを暗号化するための S 秘密鍵 3 2 4 を記憶する。サーバ 3 0 4 は更に、コンピュータテストツール 3 0 2 から受信したメッセージを復号化するためのそれぞれ 1 つ又は 2 つ以上のコンピュータテストツール 3 0 2 に関連付けられた少なくとも 1 つの C T T 公開鍵 3 2 6 を記憶する。サーバ 3 0 4 は、受信したメッセージがコンピュータテストツール 3 0 2 から送信されること、また、コンピュータテストツール 3 0 2 に送信されたメッセージがサーバ 3 0 4 によって送信されたことを認証するために、通信デバイス 3 0 6 と交換したメッセージを処理する認証モジュール 3 2 8（例えば、サーバ 3 0 4 のメモリ 2 2 8 によって記憶されたプログラムモジュール 2 1 5）を含む。

30

【 0 0 5 7 】

サーバ 3 0 4 は、診断データを処理する、及び/又は診断データを記憶デバイス 3 3 2 に記憶する診断データ処理モジュール 3 3 0（例えば、サーバ 3 0 4 のメモリ 2 2 8 によって記憶されたプログラムモジュール 2 1 5）を更に含む。記憶デバイス 3 3 2 は、サーバ 3 0 4 内、又はその周辺に含まれ得る。サーバ 3 0 4 は、コンピュータテストツール 3 0 2 を制御及び構成するための制御及び/又は構成データを生成する制御及び構成モジュール 3 3 4（例えば、サーバ 3 0 4 のメモリ 2 2 8 によって記憶されたプログラムモジュール 2 1 5）を更に含む。

40

【 0 0 5 8 】

オペレーション中、通信デバイス 3 0 6 は第 2 の通信リンク 3 1 0 を用いて第 2 のネットワーク 3 0 8 と通信し、またサーバ 3 0 4 は第 3 の通信リンク 3 1 2 を用いて第 2 のネットワーク 3 0 8 と通信する。破線で示されるように、通信リンク 3 1 0 は、断続的とすることができ、コンピュータテストツール 3 0 2 及び通信デバイス 3 0 6 はリンク 3 1 0 が壊れるように選択的に切断でき、その後、再確立され得る。同様に、破線で示されるよ

50

うに、通信リンク 312 は、断続的とすることができ、通信デバイス 306 はリンク 312 が壊れるように第 2 のネットワーク 308 との通信から選択的に切断でき、その後、再確立され得る。

【0059】

典型的な実施形態では、第 1 の通信リンクは、リンクされたコンピュータテストツール 302 及び通信デバイス 306 だけを含む第 1 のネットワークとの、例えば blue-tooth 通信又は USB ケーブルのいずれかを用いた単一の近距離無線通信リンク又は有線通信リンクである。コンピュータテストツール 302 は、診断テストを行い、時間 t_1 前に関連診断データをコンピュータテストツール 302 のローカルメモリに記憶する。コンピュータテストツール 302 及び通信デバイス 306 は、時間 t_2 では第 1 の通信リンク 310 を介して結合され得る。通信デバイス 306 は、サーバ 304 と通信するため、時間 t_3 において第 2 のネットワーク 308 と結合することができるスマートフォン又はタブレット又はラップトップである。サーバ 304 は、安定した接続を介して第 2 のネットワーク 308 と結合されるので、1 つ又は 2 つ以上のコンピュータテストツール 302 にサービスを提供することができる。一実施形態では、 t_1 、 t_2 、及び / 又は t_3 は離間された時系列順（即ち、時間において互いに離間されている）とすることができる。

10

【0060】

換言すれば、コンピュータテストツール 302 は、1 つ又は 2 つ以上の診断テストを行い、関連する診断テストデータをローカル記憶装置に記憶することができ、これらのすべては時間 t_1 の前に発生する。通信デバイス 306 を保有するユーザは、後の時間 t_2 でコンピュータテストツール 302 に近づき、近距離無線通信を用いて通信デバイス 306 をコンピュータテストツール 302 に結合することができる。診断データ、又はそのコピーは、時間 t_2 で通信デバイス 306 に転送され、通信デバイス 306 によって一時的に記憶され得る。後の時間 t_3 では、通信デバイス 306 は第 2 のネットワーク 308 に結合し、診断データをサーバ 304 に転送することができる。一実施形態では、コンピュータテストツール 302 は、時間 t_1 において第 1 のネットワーク（第 1 の通信リンク 310）を介して通信デバイス 306 に結合され得るので、 t_1 及び t_2 はほぼ同じ時間となり得る。一実施形態では、通信デバイス 306 は、時間 t_2 において第 2 のネットワーク 308 に結合され得るので、 t_2 及び t_3 はほぼ同じ時間となり得る。

20

【0061】

通信デバイス 306 がホットスポットとして使用されるか、あるいはテザーされている場合、通信リンク 310、312 を介したデータ交換は、偽物又は偽造データを送信している通信デバイス 306 になりすますデバイスによるなど、侵入に対して脆弱である可能性がある。診断システム 300 は、偽物又は偽造データの送信の脅威に対して特に脆弱であるのは、コンピュータテストツール 302 又はサーバ 304 に送信されたデータは通信デバイス 306 によって記憶され得るからである。コンピュータテストツール 302 は、通信デバイス 306 から受信したデータがサーバ 304 から起こったことを検証するとともに、コンピュータテストツール 302 から送信されたデータを認証する CTT 認証モジュール 322 を含む。同様に、サーバ 304 は、通信デバイス 306 から受信したデータがコンピュータテストツール 302 から起こったことを検証するとともに、サーバ 304 から送信されたデータを認証する S 認証モジュール 328（後述する）を含む。

30

40

【0062】

ここで図 4 ~ 図 8 を参照すると、様々な典型的な実施形態の実装を説明するフローチャートが示されている。図 4 ~ 図 8 に示すオペレーションの順序は必須ではなく、したがって原則として、様々なオペレーションは図示された順序以外で行われてもよいことに留意されたい。また、特定のオペレーションをスキップしてもよいし、異なるオペレーションを追加又は置換してもよいし、あるいは選択されたオペレーション又はオペレーションのグループを本明細書に記載する実施形態に従う別個のアプリケーションにおいて行ってもよい。

【0063】

50

図4は、診断データをコンピュータテストツール302から通信デバイス306に送信する際に、開示の方法に従って行われるオペレーションのフローチャートを示す。オペレーション401では、CTT秘密鍵318が記憶される。オペレーション402では、診断デバイス316は物理的実体に関連付けられた特性を測定し、診断データを出力する。オペレーション404では、診断デバイス316によって出力された診断データが、コンピュータテストツール302によって（例えば、キャッシュ232又は記憶システム234に）記憶される。オペレーション406では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク310を介してコンピュータテストツール302と通信デバイス306との結合の確立を含むことができる。トリガは、更に、例えば、コンピュータテストツール302及び通信デバイス306のいずれか又はそれらの組み合わせによって提出された要求を含む、あるいは必要とする場合がある。オペレーション408では、転送されるべき記憶された診断データは、CTT秘密鍵318を用いてCTT認証モジュール322によって暗号化される。オペレーション410では、暗号化された診断データが、通信デバイス306を介してサーバ304に送信されるように、結合された通信デバイス306に送信されており、ここで通信デバイス306はデータを復号化できないが、サーバ304はサーバ304がデータを復号化できるようにする復号化鍵（例えば、CTT公開鍵）を記憶する。

10

【0064】

図5は、制御及び/又は構成データをコンピュータテストツール302によってサーバ304から受信する際に、開示の方法に従って行われるオペレーションのフローチャートを示す。オペレーション501では、S公開鍵318が記憶される。オペレーション502では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク310を介してコンピュータテストツール302と通信デバイス306との結合の確立を含むことができる。トリガは、例えば、コンピュータテストツール302及び通信デバイス306のいずれか又はそれらの組み合わせによって提出された要求を更に含む、あるいは必要とする場合がある。オペレーション504では、暗号化された制御及び/又は構成データを、結合された通信デバイス306から受信し、ここで暗号化された制御及び/又は構成データは、サーバ304から通信デバイス306に送信されたものであり、通信デバイス306は暗号化された制御及び/又は構成データを復号化する鍵を持たない。オペレーション506では、暗号化された制御及び/又は構成データは、S公開鍵320を用いてCTT認証モジュール322によって復号化される。オペレーション508では、制御及び/又は構成データは、コンピュータテストツール302を制御又は構成する（例えば、ブリック（brick）する（無効にする）、アンブリック（unbrick）する（再有効化する、更新する））ように処理される。

20

30

【0065】

図6は、コンピュータテストツール302又はサーバ304と通信デバイス306によりデータを交換する際の、開示の方法に従って行われるオペレーションのフローチャートを示す。オペレーション602では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク310を介してコンピュータテストツール302と通信デバイス306と、又は通信リンク312を介して通信デバイス306とサーバ304とのうち一方の結合の確立を含むことができる。トリガは、例えば、コンピュータテストツール302、サーバ304、及び通信デバイス306のいずれか又はそれらの組み合わせによって提出された要求を更に含む、又は必要とする場合がある。オペレーション604では、暗号化されたデータ（診断データ又は制御及び/若しくは構成データ）をコンピュータテストツール302又はサーバ304のうち一方から受信する。通信デバイス306は受信したデータを復号化できない。

40

【0066】

オペレーション606では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク310を介してコンピュータテストツール302と通信デバイス306との、又は通信リンク312を介して通信デバイス306とサーバ304とのうち

50

他方の結合の確立を含むことができる。トリガは、例えば、コンピュータテストツール 302、サーバ 304、及び通信デバイス 306 のいずれか又はそれらの組み合わせによって提出された要求を更に含む、又は必要とする場合がある。オペレーション 608 では、受信したデータは、確立された結合を有する、コンピュータテストツール 302 とサーバ 304 のうち他方に送信される。データは、そのデータを受信したコンピュータテストツール 302 又はサーバ 304 によってそのデバイス用に記憶された公開鍵を用いて復号化され得る。

【0067】

図 7 は、診断データをサーバ 304 により通信デバイス 306 を用いて受信する際の、開示の方法に従って行われるオペレーションのフローチャートを示す。オペレーション 701 では、CTT 公開鍵 318 が記憶される。オペレーション 702 では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク 312 を介して通信デバイス 306 とサーバ 304 との結合の確立を含むことができる。トリガは、例えば、サーバ 304 及び通信デバイス 306 のいずれか又はそれらの組み合わせによって提出された要求を更に含む、又は必要とする場合がある。オペレーション 704 では、暗号化された診断データを受信する。暗号化された診断データは通信デバイス 306 によってサーバ 304 に送信されたものであり、通信デバイス 306 は暗号化された診断データを復号化することができない（例えば、公開鍵を持たない）。オペレーション 706 では、診断データは、CTT 公開鍵 320 を用いて S 認証モジュール 328 によって復号化される。オペレーション 708 では、復号化された診断データは、診断データ処理モジュール 330 によって処理され、かつ/又は記憶デバイス 332 に記憶される。

10

20

【0068】

図 8 は、制御及び/又は構成データをサーバ 304 によって通信デバイス 306 を介してコンピュータテストツール 302 に送信する際に、開示の方法に従って行われるオペレーションのフローチャートを示す。オペレーション 801 では、S 秘密鍵 324 が記憶される。オペレーション 802 では、待機ループがトリガが発生するまで行われ、ここでトリガは、例えば、通信リンク 312 を介してコンピュータテストツール 306 とサーバ 304 との結合の確立を含むことができる。トリガは、例えば、サーバ 304 及び通信デバイス 306 のいずれか又はそれらの組み合わせによって提出された要求を更に含む、又は必要とする場合がある。オペレーション 804 では、例えば、制御及び構成モジュール 334 によって生成された制御及び/又は構成データは、S 秘密鍵 324 を用いて S 認証モジュール 328 によって暗号化される。オペレーション 804 では、暗号化された制御及び/又は構成データは、通信デバイス 306 に送信されており、ここで通信デバイス 306 は暗号化された制御及び/又は構成データを復号化できないが、コンピュータテストツール 302 は、コンピュータテストツール 302 に暗号化された制御及び/又は構成データを復号化できるようにする復号化鍵（例えば、S 公開鍵）を記憶する。

30

【0069】

図 9 は、複数の通信デバイス 306 a ~ 306 n が設けられた開示の別の実施形態のフローチャートを示す。通信デバイス 306 a ~ 306 n は、各通信リンク 310 a ~ 310 n により、コンピュータテストツール 202 に、また各通信リンク 312 a ~ 312 n を介してサーバ 304 に結合される。

40

【0070】

オペレーション中は、CTT 認証モジュール 322 又は S 認証モジュール 328 がデータメッセージを暗号化する際、非暗号化識別タグ（例えば、英数字タグ）をメッセージに追加する。メッセージの複数のコピーは、通信デバイス 306 a ~ 306 n のうち複数のデバイスに送信され得る。一実施形態では、メッセージのコピーのうち 1 つがサーバ 304 によって受信されるとき、サーバ 304 はメッセージのうち 1 つだけを復号化、処理、及び/又は記憶できるが、他のコピーは無視されかつ/又は削除され得る。一実施形態では、メッセージの第 1 のコピーがサーバ 304 によって受信されるとき、サーバ 304 は暗号化された受信通知をコンピュータテストツール 302 に送信することができる。サー

50

バ 3 0 4 及び / 又はコンピュータテストツール 3 0 2 は、例えば、この受信通知に回答して、暗号化されていない「すべての複製を削除する (delete all duplicates)」(DAD) メッセージを、コンピュータテストツール 3 0 2 が結合することができる通信デバイス 3 0 6 a ~ 3 0 6 n に送信することができる。DAD メッセージは、通信デバイス 3 0 6 a ~ 3 0 6 n に、それが記憶又は処理している ID を有するデータメッセージのあらゆるコピーを削除するように命令する。したがって、DAD メッセージに回答する通信デバイス 3 0 6 a ~ 3 0 6 n は、サーバ 3 0 4 によってすでに受信されたメッセージのコピーをもはや記憶又は送信しないことになる。

【 0 0 7 1 】

同様に、一実施形態では、メッセージのコピーのうち 1 つがコンピュータテストツール 3 0 2 によって受信されるとき、コンピュータテストツール 3 0 2 はメッセージのうち 1 つだけを復号化、処理、及び / 又は記憶できるが、他のコピーは無視され、かつ / 又は削除され得る。一実施形態では、メッセージの第 1 のコピーがコンピュータテストツール 3 0 2 によって受信されるとき、コンピュータテストツール 3 0 2 は暗号化された受信通知をサーバ 3 0 4 に送信することができる。受信通知に回答して、サーバ 3 0 4 は暗号化されていない DAD メッセージを、コンピュータテストツールとの結合の追跡履歴を有する選択された通信デバイス 3 0 6 a ~ 3 0 6 n に送信する。DAD メッセージの受信に回答して、選択された通信デバイス 3 0 6 a ~ 3 0 6 n は、そのデバイス 3 0 6 によって記憶され、又は処理されている ID を有するデータメッセージのあらゆるコピーを削除する。したがって、選択された通信デバイス 3 0 6 a ~ 3 0 6 n は、コンピュータテストツール 3 0 2 によってすでに受信されたメッセージのコピーをもはや記憶又は送信しない。この実施形態では、サーバ 3 0 4 は、コンピュータテストツール 3 0 2 とのデータメッセージの交換履歴を有する通信デバイス 3 0 6 の識別を追跡及び記憶することができる。

【 0 0 7 2 】

一実施形態では、コンピュータテストツール 3 0 2 又はサーバ 3 0 6 がデータを暗号化するとき、1 回使用のインジケータをデータメッセージに追加する。この 1 回使用のインジケータは、データを復号化するモジュール (例えば、CTT 認証モジュール 3 2 2 又は S 認証モジュール 3 2 8) に、そのデータが 1 回だけしか復号化又は処理できないことを示す。

【 0 0 7 3 】

* * 例えば、サーバ 3 0 6 は、1 回使用のメッセージをコンピュータテストツール 3 0 2 に送信し、特別の機能、ターンオン、ターンオフを実行するか、あるいは後続のメッセージが受信されるまで、それ自体をブリックすることができる。1 回使用のメッセージはシーケンス番号で暗号化されるので、この 1 回使用のメッセージは、例えば、コンピュータテストツール 3 0 2 をターンオン又はターンオフするために再利用することができない。暗号化されたシーケンス番号は、単一の正当な 1 回使用のメッセージの記憶及び再利用を防止する。例えば、ユーザが特定の特別な特徴の 1 週間の使用を購入するとき、サーバ 3 0 6 は、コンピュータテストツール 3 0 2 にシーケンス番号で暗号化された 1 回使用の「この特徴をオンするメッセージ (turn on this feature message)」を送信することができる。1 週間が終わると、コンピュータテストツール 3 0 2 は自動的にその特徴を遮断する。シーケンス番号は、ユーザが、特別な機能のもう 1 週間の使用を獲得するために、元のメッセージを再利用する (例えば、元のメッセージをコンピュータテストツール 3 0 2 に再生する) のを防止する。

【 0 0 7 4 】

一実施形態では、CTT 認証モジュール 3 2 2 及び S 認証モジュール 3 2 8 は、「有効期限 (time to live)」(TTL) 情報を、コンピュータテストツール 3 0 2 及びサーバ 3 0 4 によって交換されたデータメッセージに添加する。TTL 情報は、満了期日を示す。データメッセージに関連する満了データが経過すると、メッセージを記憶又は処理する任意の通信デバイス 3 0 6 a ~ 3 0 6 n は、メッセージを削除する。メッセージの寿命を制限するための TTL 情報の使用は、同じメッセージが 1 回以上、様々なパスを介して通

10

20

30

40

50

信リンク310a~310n及び/又は312a~312nを通して送信され得る機会を減少することができる。

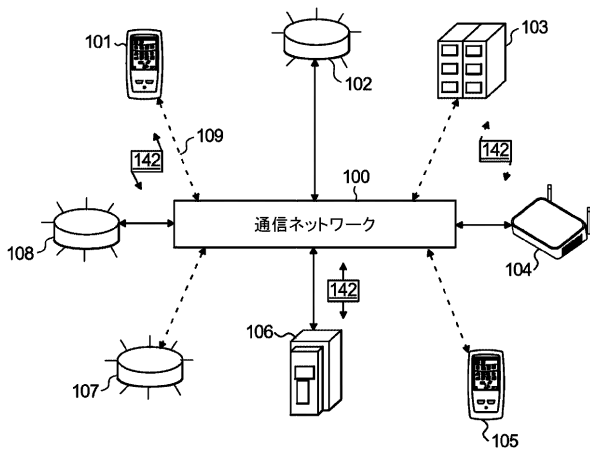
【0075】

上述した特定の例示の実施形態では、本明細書に記載した様々な非限定的な実施形態は、特別の用途のために別々に用いられ、組み合わせて、あるいは選択して組み合わせてもよいことは理解されよう。更に、上記非限定的な実施形態の様々な特徴の一部は、他の記載した特徴を対応して使用せずに用いられる場合がある。したがって、前述の説明は、本発明の原理、教示及び典型的な実施形態の単なる説明であって、その限定のためではないと見なすべきである。

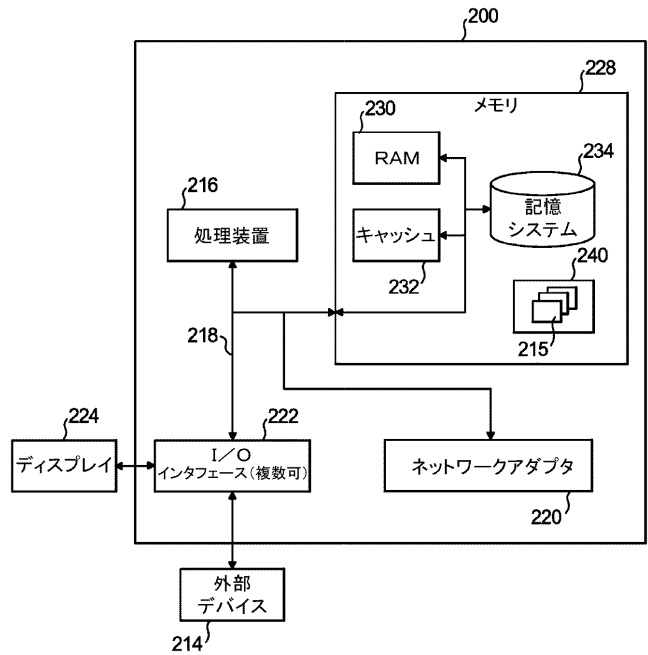
【0076】

上述した配置は例示の実施形態の原理の用途の単なる説明であることが理解されよう。多くの変更態様及び代替の構成が、例示の実施形態の範囲から逸脱することなく当業者によって考案することができ、添付する特許請求の範囲はかかる変更態様及び構成を包摂することを目的とするものである。

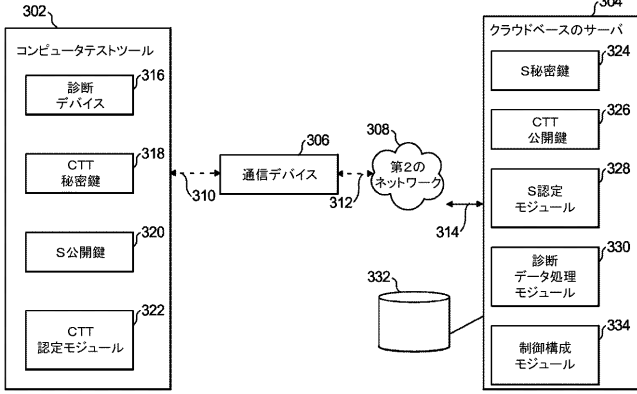
【図1】



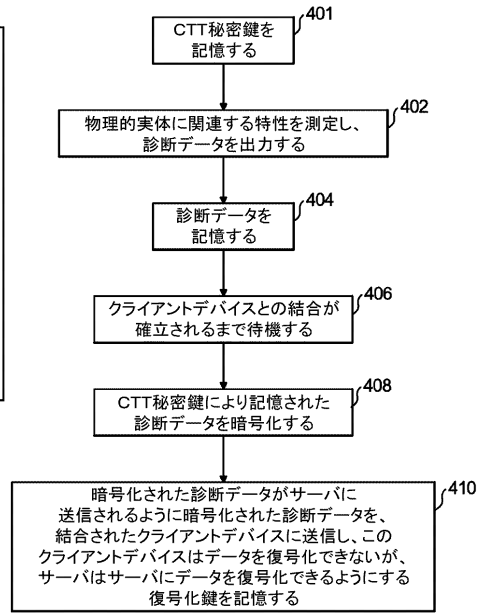
【図2】



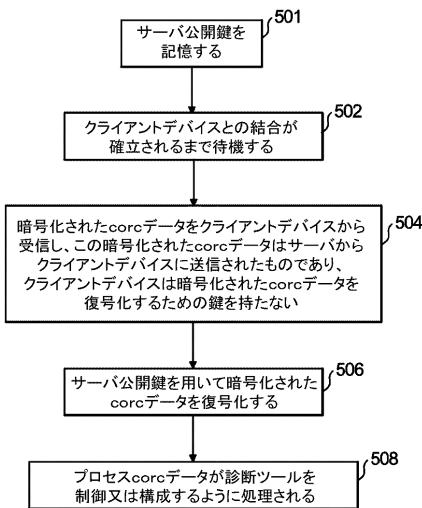
【 図 3 】



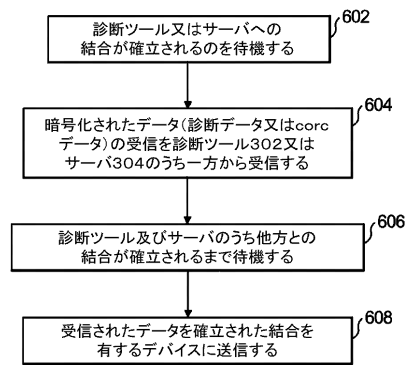
【 図 4 】



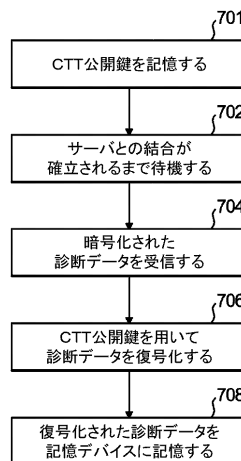
【 図 5 】



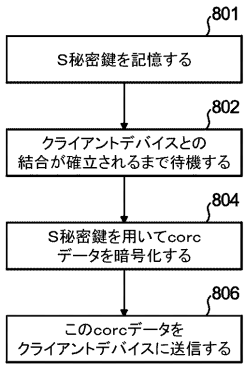
【 図 6 】



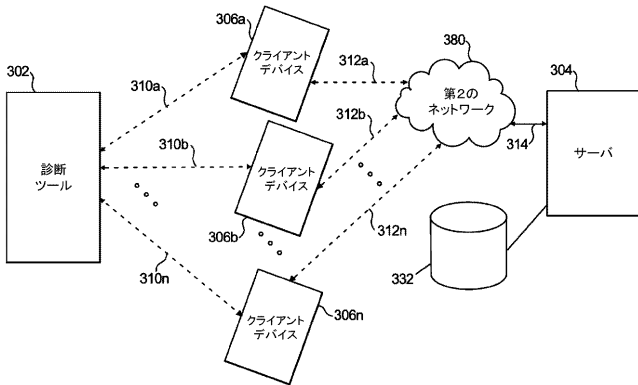
【 図 7 】



【 図 8 】



【 図 9 】



フロントページの続き

(51)Int.Cl. F I テーマコード(参考)
G 0 6 F 21/60 (2013.01) G 0 6 F 11/30 1 4 0 A
G 0 6 F 21/60 3 6 0

(72)発明者 クリントン・ジェイ・ウートン
アメリカ合衆国 ワシントン州 9 8 2 5 8 レイク スティーブンス ノースイースト テンス
・ストリート 8 2 2 1

Fターム(参考) 5B042 GA12 GC20 MA09 MA19 MC38
5J104 AA08 AA16 EA04 LA03 NA02 NA37 PA07
5K201 AA08 CB17 CC01 EB07 EC06 ED04 ED05 ED07 EE06 FB08

【外国語明細書】

2017169190000001.pdf