(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6901850号
(P6901850)
(45)発行日　令和3年7月14日(2021.7.14)　(24)登録日　令和3年6月22日(2021.6.22)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
H04L	9/08	(2006.01)	H04L	9/00	601F
H04M	11/00	(2006.01)	H04M	11/00	302
H04M	3/00	(2006.01)	H04M	3/00	E
G06F	11/30	(2006.01)	G06F	11/30	158

請求項の数 18　外国語出願　(全 22 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)
(65)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)
審査請求日　令和1年12月13日 (2019.12.13)
(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・地域又は機関
米国 (US)

(73)特許権者　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　スコッツデイル　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)【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テストデータを生成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、
該当する通信回線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とそれぞれが通信しており、且つ、テストされている前記コンピュータネットワークとは異なり、前記該当する通信回線とも異なる通信ネットワークに無線で通信している、複数の通信デバイスと、
前記通信ネットワークと通信しているクラウドベースのサーバと、を備えるシステムであって、
前記少なくとも１つのコンピュータテストツールが、
前記テストデータを暗号化して暗号化されたテストデータを生成し、前記テストデータの非暗号化識別タグを前記暗号化されたテストデータに添加し、
前記非暗号化識別タグを有する前記暗号化されたテストデータのコピーを、前記該当する通信回線を介して、前記複数の通信デバイスのそれぞれに提供し、
前記クラウドベースのサーバから、前記クラウドベースのサーバが前記暗号化されたテストデータを受信したとの受信通知を受信することに応答して、前記複数の通信デバイスのそれぞれに命令を出し、前記非暗号化識別タグを有する前記暗号化されたテストデータを削除する、コンピュータ命令を実行するプロセッサを含み、

前記複数の通信デバイスのそれぞれの該当する通信デバイスが、
前記該当する通信デバイスが、前記通信ネットワークを介して前記クラウドベースのサーバと通信しているか否かを決定し、
前記該当する通信デバイスが前記クラウドベースのサーバと通信している前記該当する通信デバイスによる決定に応答して、前記該当する通信デバイスから前記クラウドベースのサーバに前記暗号化されたテストデータを送信し、
前記該当する通信デバイスによる前記少なくとも１つのコンピュータテストツールからの命令の受信に応答して、前記非暗号化識別タグを有する前記暗号化されたテストデータを削除して、前記該当する通信デバイスが前記クラウドベースのサーバに前記暗号化されたテストデータをもはや送信しないようにする、コンピュータ命令を実行するプロセッサを含み、
前記クラウドベースのサーバが、
前記複数の通信デバイスの一つから前記暗号化されたテストデータを復号化し、
前記少なくとも１つのコンピュータテストツールに前記受信通知を提供する、コンピュータ命令を実行するプロセッサを含む、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の前記プロセッサが、前記通信ネットワーク及び前記複数の通信デバイスの少なくとも１つ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コンピュータ命令を更に実行する、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の前記プロセッサが、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コンピュータ命令を更に実行する、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暗号化されたデータが、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の前記プロセッサが、前記複数の通信デバイスの少なくとも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１つ又は２つ以上の診断テストから生じる前記テストデータをキャッシュするコンピュータ命令を更に実行する、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）、Ｗｉ Ｆｉ、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】
前記複数の通信デバイスのそれぞれの該当する通信デバイスのプロセッサが、前記該当する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前記暗号化されたテストデータをキャッシュするコンピュータ命令を更に実行する、請求項１に記載のシステム。
【請求項９】
前記複数の通信デバイスが、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】
前記クラウドベースのサーバの前記プロセッサは、前記複数の通信デバイスのそれぞれに、制御又は構成データのコピーを送信する第１のコンピュータ命令を更に実行し、それぞれのコピーは、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、
前記制御又は構成データを受信することに応答して、前記少なくとも１つのコンピュータテストツールの前記プロセッサは、前記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する第２のコンピュータ命令を更に実行し、
前記受信通知の受信に応答して、前記クラウドベースのサーバの前記プロセッサは前記同一の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、前記複数の通信デバイスのそれぞれに送信する第１のコンピュータ命令を更に実行する、
請求項３に記載のシステム。
【請求項１１】
前記少なくとも１つのコンピュータテストツールの前記プロセッサは、前記複数の通信デバイスのうちいずれかによって記憶された前記暗号化されたテスト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第１の時間を示す前記暗号化されたテストデータに第１の満了時間を添加する第１のコンピュータ命令を更に実行し、
前記クラウドベースのサーバの前記プロセッサは、前記複数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に送信された制御又は構成データに、前記複数の通信デバイスのうちいずれかによって記憶された前記制御又は構成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第２の時間を示す第２の満了時間を添加する第２のコンピュータ命令を更に実行する、請求項１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、前記複数の通信デバイス、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構成される、請求項１１に記載のシステム。
【請求項１３】
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テストデータを生成し、
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て暗号化されたテストデータを生成し、
前記暗号化されたテストデータに、前記テストデータを識別する非暗号化識別タグを添加し、
テストされているコンピュータネットワークとは異なる通信リンクを介して、前記非暗号化識別タグを有する前記暗号化されたテストデータのコピーを複数の通信デバイスに送信し、前記暗号化されたテストデータの前記コピーは、前記コンピュータテストツールと前記複数の通信デバイスと前記テストされているコンピュータネットワークとの間の前記通信リンクとは異なるワイヤレスネットワークを介して、前記複数の通信デバイスの少なくとも１つと通信して、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おり、
前記クラウドベースのサーバから、前記クラウドベースのサーバが前記暗号化されたテストデータを受信したとの受信通知を受信することに応答して、前記複数の通信デバイスのそれぞれに命令を出し、前記非暗号化識別タグを有する前記暗号化されたテストデータを削除して、前記複数の通信デバイスが前記クラウドベースのサーバに前記暗号化された

テストデータをもはや送信しないようにする、コンピュータテストツール。
【請求項１４】
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複数の通信デバイスの少なくとも１つを介して受信する、請求項１３に記載の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の前記プロセッサは、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コンピュータ命令を更に実行する、請求項１４に記載のコンピュータテストツール。
【請求項１６】
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が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前記暗号化されたデータを復号化する、請求項１５に記載のコンピュータテストツール。
【請求項１７】
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複数の通信デバイスの少なくとも１つと通信リンクを確立するまで、前記テストデータをキャッシュする、請求項１３に記載のコンピュータテストツール。
【請求項１８】
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、
コンピュータテストデバイスのオペレーションに関連した制御又は構成データを暗号化し、コンピュータネットワーク上で診断テストを実行して暗号化された制御又は構成データを生成し、
第２の通信接続を介したコンピュータテストデバイスに進行するための該当する第１の通信接続を介した複数の通信デバイスのそれぞれに、前記暗号化された制御又は構成データのコピーを送信し、前記第１の通信接続と前記第２の通信接続が、前記コンピュータテストデバイスによってテストされている前記コンピュータネットワークとは異なっており、
前記コンピュータテストデバイスが前記暗号化された制御又は構成データを受信したとの受信通知を受信することに応答して、前記複数の通信デバイスのそれぞれに命令を出し、前記暗号化された制御又は構成データの前記コピーを削除して、前記複数の通信デバイスが前記コンピュータテストデバイスに前記暗号化された制御又は構成データをもはや送信しないようにし、
該当する第１の通信接続を介した少なくとも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通信が確立されると、暗号化されたテストデータを前記複数の通信デバイスの少なくとも１つの通信デバイスから受信し、テストデータが前記コンピュータテストデバイスによって前記コンピュータネットワーク上で行われる前記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され、及び暗号化されて暗号化されたテストデータを生成し、前記クラウドベースのサーバで復号化され、前記複数の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該当する第２の通信接続が確立されると、前記複数の通信デバイスに前記コンピュータテストデバイスによって送信され、
前記暗号化されたテストデータを復号化する、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。
【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
【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スセスを提供するために、モバイルフォン、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ある。
【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。
【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。
【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。

【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。

【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することができ、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応答して、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。受信通知の受信に応答して、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つの通信デバイスに送信することができる。

【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。

【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。

【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。

【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に、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り得る、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。

【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ーキ（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。

【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。

【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。

【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もよい。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、電気的、磁気的、光学的、電磁気的、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気的接続、ポータブルコンピュータディスケット、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。

【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、電磁気的、光学的、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、Ｊ

ａｖａ（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。

【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。

【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ン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。

【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。

【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。

【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。

【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、ネットワーキング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関係する各デバイスは、一対の暗号鍵（公開暗号化鍵及び秘密復号化鍵）を備えている。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。

【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。

【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。
【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。
【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（例えば、プログラムモジュール２１５）を含む。
【００５４】
別の実施形態では、コンピュータテストツール３０２は、通信デバイス３０６にテザーされており、通信リンク３１０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３０６は、通信リンク３１０を介したコンピュータテストツール３０２とのデータの交換、並びに通信３１２及びインターネットを介したサーバ３０４とのデータの交換を含む、コンピュータテストツール３０２とサーバ３２４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３０６は、通信リンク３１０が動作しているとき、コンピュータテストツール３０２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３１２が動作しているとき、記憶された診断データをサーバ３０４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２１５）を含む。一実施形態では、通信リンク３１０及び３１２の両方が動作しているとき、通信デバイス３０６は、診断データの記憶を差し控えることができる。
【００５５】
サーバ３０４は、（例えば、ネットワークアダプタ２２０を介して）第２のネットワーク３０８に通信リンク３１４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３０６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３１４は、動作時間中、通信デバイス３０６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３０４は、通信デバイス３０６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（ｃｏｒｃ）メッセージをコンピュータテストツール３０２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（２４／７）のうち任意の時間を含むことができる。
【００５６】
サーバ３０４は、（例えば、メモリ２２８に）サーバ３０４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Ｓ秘密鍵３２４を記憶する。サ

ーバ３０４は更に、コンピュータテストツール３０２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３０２に関連付けられた少なくとも１つのＣＴＴ公開鍵３２６を記憶する。サーバ３０４は、受信したメッセージがコンピュータテストツール３０２から送信されること、また、コンピュータテストツール３０２に送信されたメッセージがサーバ３０４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と交換したメッセージを処理する認証モジュール３２８（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。

【００５７】

サーバ３０４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３３２に記憶する診断データ処理モジュール３３０（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）を更に含む。記憶デバイス３３２は、サーバ３０４内、又はその周辺に含まれ得る。サーバ３０４は、コンピュータテストツール３０２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３３４（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）を更に含む。

【００５８】

オペレーション中、通信デバイス３０６は第２の通信リンク３１０を用いて第２のネットワーク３０８と通信し、またサーバ３０４は第３の通信リンク３１２を用いて第２のネットワーク３０８と通信する。破線で示されるように、通信リンク３１０は、断続的とすることができ、コンピュータテストツール３０２及び通信デバイス３０６はリンク３１０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ｔ１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ｔ２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ｔ３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モバイル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、ｔ１、ｔ２、及び／又はｔ３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。

【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ｔ１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ｔ２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ｔ２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ｔ３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ｔ１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、ｔ１及びｔ２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ｔ２において第２のネットワーク

３０８に結合され得るので、ｔ２及びｔ３はほぼ同じ時間となり得る。

【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。

【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】

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。

【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。

【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。

【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。

【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。

【００６９】

図９は、複数の通信デバイス３０６ａ～３０６ｎ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３０６ａ～３０６ｎは、各通信リンク３１０ａ～３１０ｎ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３１２ａ～３１２ｎを介してサーバ３０４に結合される。

【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）をメッセージに添加する。メッセージの複数のコピーは、通信デバイス３０６ａ～３０６ｎ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。サーバ３０４及び／又はコンピュータテストツール３０２は、例えば、この受信通知に応答して、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３０２が結合することができる通信デバイス３０６ａ～３０６ｎに送信することができる。ＤＡＤメッセージは、通信デバイス３０６ａ～３０６ｎ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メッセージに応答する通信デバイス３０６ａ～３０６ｎは、サーバ３０４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。

【００７１】

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３０２によって受信されるとき、コンピュータテストツール３０２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３０２によって受信されるとき、コンピュータテストツール３０２は暗号化された受信通知をサーバ３０４に送信することができる。受信通知に応答して、サーバ３０４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３０６ａ～３０６ｎに送信する。ＤＡＤメッセージの受信に応答して、選択された通信デバイス３０６ａ～３０６ｎは、そのデバイス３０６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３０６ａ～３０６ｎは、コンピュータテストツール３０２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３０４は、コンピュータテストツール３０２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３０６の識別を追跡及び記憶することができる。

【００７２】

一実施形態では、コンピュータテストツール３０２又はサーバ３０６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３２２又はＳ認証モジュール３２８）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。

【００７３】

＊＊例えば、サーバ３０６は、１回使用のメッセージをコンピュータテストツール３０２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３０２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３０６は、コンピュータテストツール３０２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３０２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３０２に再生する）のを防止する。

【００７４】

一実施形態では、ＣＴＴ認証モジュール３２２及びＳ認証モジュール３２８は、「有効期限（time to live）」（ＴＴＬ）情報を、コンピュータテストツール３０２及びサーバ３０４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３０６ａ～３０６ｎ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。

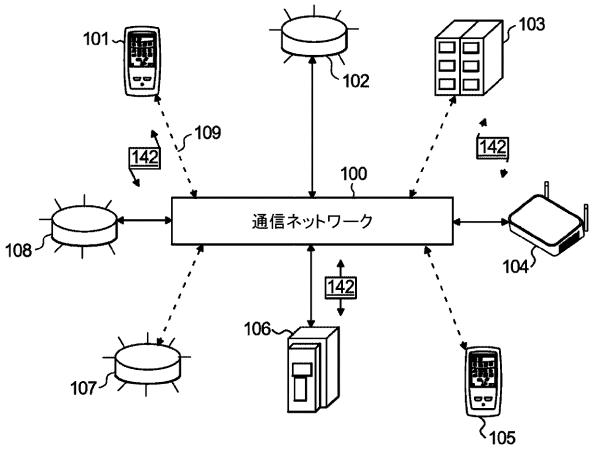
【００７５】

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。

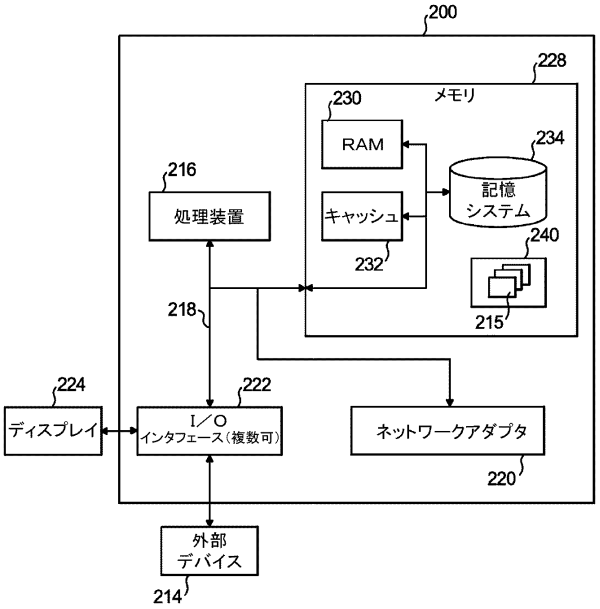
【００７６】

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。

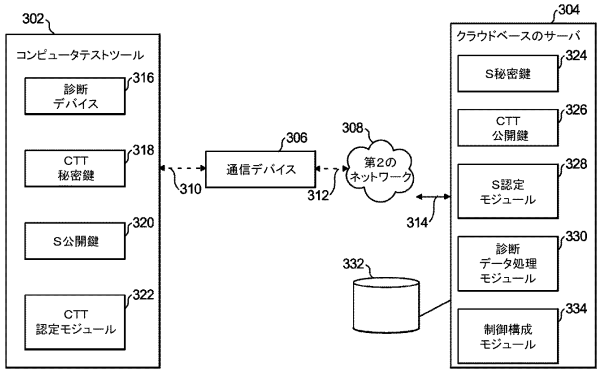
【図１】


101
102
103
109
142
142
100
通信ネットワーク
108
104
142
106
107
105

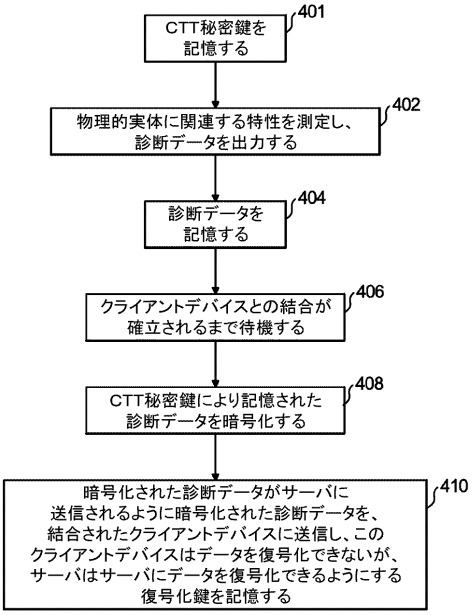
【図２】


200
228
メモリ
230
RAM
234
記憶
システム
216
処理装置
キャッシュ
240
232
215
218
224
222
ディスプレイ
I／O
インタフェース（複数可）
ネットワークアダプタ
220
外部
デバイス
214

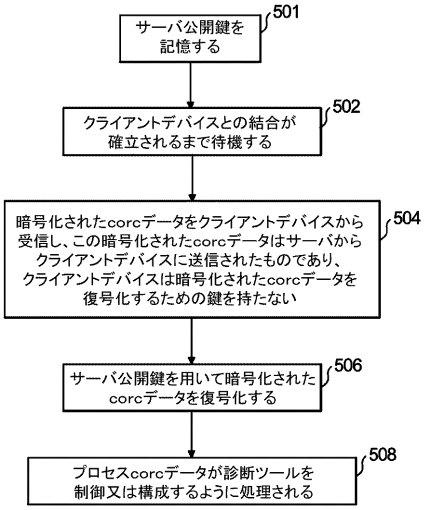
【図３】


302
コンピュータテストツール
診断
デバイス
316
CTT
秘密鍵
318
S公開鍵
320
CTT
認定モジュール
322
310
306
通信デバイス
308
第2の
ネットワーク
312
314
304
クラウドベースのサーバ
S秘密鍵
324
CTT
公開鍵
326
S認定
モジュール
328
診断
データ処理
モジュール
330
制御構成
モジュール
334
332

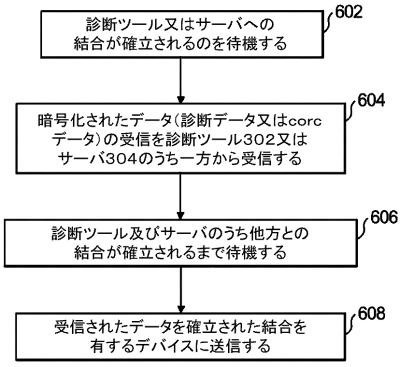
【図４】


CTT秘密鍵を
記憶する
401
物理的実体に関連する特性を測定し、
診断データを出力する
402
診断データを
記憶する
404
クライアントデバイスとの結合が
確立されるまで待機する
406
CTT秘密鍵により記憶された
診断データを暗号化する
408
暗号化された診断データがサーバに
送信されるように暗号化された診断データを、
結合されたクライアントデバイスに送信し、この
クライアントデバイスはデータを復号化できないが、
サーバはサーバにデータを復号化できるようにする
復号化鍵を記憶する
410

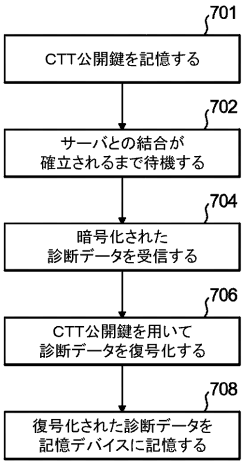
【図５】


501
サーバ公開鍵を記憶する
502
クライアントデバイスとの結合が確立されるまで待機する
504
暗号化されたcorcデータをクライアントデバイスから受信し、この暗号化されたcorcデータはサーバからクライアントデバイスに送信されたものであり、クライアントデバイスは暗号化されたcorcデータを復号化するための鍵を持たない
506
サーバ公開鍵を用いて暗号化されたcorcデータを復号化する
508
プロセスcorcデータが診断ツールを制御又は構成するように処理される

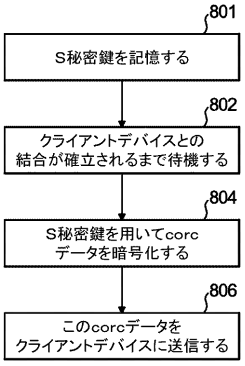
【図６】


602
診断ツール又はサーバへの結合が確立されるのを待機する
604
暗号化されたデータ(診断データ又はcorcデータ)の受信を診断ツール302又はサーバ304のうち一方から受信する
606
診断ツール及びサーバのうち他方との結合が確立されるまで待機する
608
受信されたデータを確立された結合を有するデバイスに送信する

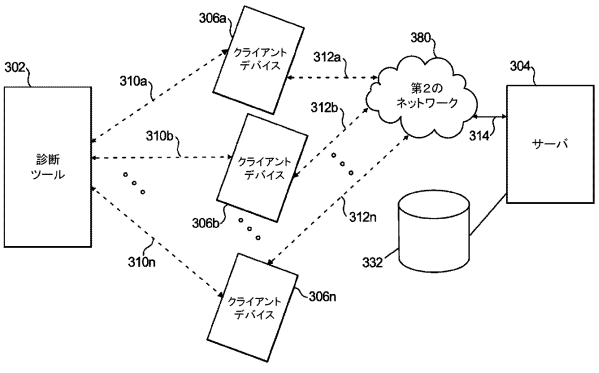
【図７】


701
CTT公開鍵を記憶する
702
サーバとの結合が確立されるまで待機する
704
暗号化された診断データを受信する
706
CTT公開鍵を用いて診断データを復号化する
708
復号化された診断データを記憶デバイスに記憶する

【図８】


801
S秘密鍵を記憶する
802
クライアントデバイスとの結合が確立されるまで待機する
804
S秘密鍵を用いてcorcデータを暗号化する
806
このcorcデータをクライアントデバイスに送信する

【図９】


306a
クライアントデバイス
312a
380
第2のネットワーク
304
サーバ
302
診断ツール
310a
310b
クライアントデバイス
312b
314
306b
312n
332
310n
クライアントデバイス
306n

フロントページの続き

(51)Int.Cl. F I
G06F 21/60 (2013.01) G06F 11/30 140A
G06F 21/60 360

(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 98258 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 8221

審査官 岸野 徹

(56)参考文献 国際公開第2014／145168（WO, A1）
米国特許出願公開第2015／0106616（US, A1）
米国特許出願公開第2014／0281484（US, A1）
特表2017－527036（JP, A）
特表2016－524197（JP, A）

(58)調査した分野(Int.Cl., DB名)
H04L 9／32
G06F 11／30
G06F 21／60
H04L 9／08
H04M 3／00
H04M 11／00