(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6367375号
(P6367375)
(45)発行日　平成30年8月1日(2018.8.1)　(24)登録日　平成30年7月13日(2018.7.13)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B

請求項の数 39 (全 18 頁)

(21)出願番号	特願2016-571026 (P2016-571026)
(86)(22)出願日	平成27年6月2日 (2015.6.2)
(65)公表番号	特表2017-524287 (P2017-524287A)
(43)公表日	平成29年8月24日 (2017.8.24)
(86)国際出願番号	PCT/US2015/033816
(87)国際公開番号	WO2015/187718
(87)国際公開日	平成27年12月10日 (2015.12.10)
審査請求日	平成29年1月19日 (2017.1.19)
(31)優先権主張番号	61/997,422
(32)優先日	平成26年6月2日 (2014.6.2)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	61/997,450
(32)優先日	平成26年6月2日 (2014.6.2)
(33)優先権主張国	米国 (US)

(73)特許権者　316006141
アイデバイシーズ　エルエルシー
アメリカ合衆国　コネチカット　シムズバリー　ロード　エイボン　１３６　ビルディング　１２
(74)代理人　110001210
特許業務法人ＹＫＩ国際特許事務所
(72)発明者　ジャコビッチ　ブラダン
アメリカ合衆国　カリフォルニア　サンフランシスコ　ヴァン　ネス　アベニュー　６０１　イー８４１

審査官　宮島　郁美

最終頁に続く

(54)【発明の名称】リンキングアドレスを用いたネットワーク上でのセキュア通信のためのシステムと方法

(57)【特許請求の範囲】
【請求項１】
セキュア通信のためのシステムにおいて、
ネットワーク上で複数の電子機器と電子通信するコンピュータシステムと、
前記コンピュータシステムと電子通信するデータベースと、
前記コンピュータシステムに保存され、それによって実行されるエンジンと、
を含み、
前記エンジンは、
前記ネットワーク上で第一の電子機器からデータパケットを電子的に受信し、
前記データパケットを処理して、その中に含まれる少なくとも３２ビットであるリンキングアドレスとペイロードを特定し、
前記リンキングアドレスと前記ペイロードを保存し、
第二の電子機器からの前記リンキングアドレスを電子的に受信し、
前記ネットワーク上で前記データパケットを前記第二の電子機器に電子的に送信するように構成され、なされていることを特徴とするシステム。
【請求項２】
請求項１に記載のシステムにおいて、
前記リンキングアドレスは少なくとも１２８ビットであることを特徴とするシステム。
【請求項３】
請求項１～２の何れか１項に記載のシステムにおいて、

前記エンジンは、前記第一の電子機器と前記第二の電子機器の情報を特定することと無関係であることを特徴とするシステム。
【請求項４】
請求項１～３の何れか１項に記載のシステムにおいて、
前記第一の電子機器と前記第二の電子機器は、前記エンジンが前記データパケットを受信する前に前記リンキングアドレスが一致するように相互にペアリングされることを特徴とするシステム。
【請求項５】
請求項１～４の何れか１項に記載のシステムにおいて、
前記エンジンにより受信された前記データパケットは、暗号化されたデータパケットであり、前記エンジンは、前記暗号化されたデータパケットを復号することを特徴とするシステム。
【請求項６】
請求項５に記載のシステムにおいて、
復号された前記データパケットの前記ペイロードは暗号化されたペイロードであることを特徴とするシステム。
【請求項７】
請求項１～６の何れか１項に記載のシステムにおいて、
前記ペイロードは、暗号化されたペイロードであり、前記第二の電子機器に送信される時に暗号化されたままであることを特徴とするシステム。
【請求項８】
請求項１～７の何れか１項に記載のシステムにおいて、
前記データパケットは役割識別子を含むことを特徴とするシステム。
【請求項９】
請求項１～８の何れか１項に記載のシステムにおいて、
前記エンジンは、前記データパケットを前記第二の電子機器に送信する前に前記データパケットを暗号化することを特徴とするシステム。
【請求項１０】
請求項１～９の何れか１項に記載のシステムにおいて、
前記エンジンは、前記第一の電子機器から前記データパケットと共に固有のブラインド証明書を受信することを特徴とするシステム。
【請求項１１】
請求項１～１０の何れか１項に記載のシステムにおいて、前記エンジンは、前記第二の電子機器から前記リンキングアドレスを受信したことに少なくとも部分的に応答して、前記ペイロードを前記第二の電子機器に送信することを判断するようにさらに構成され、なされていることを特徴とするシステム。
【請求項１２】
請求項１～１１の何れか１項に記載のシステムにおいて、前記リンキングアドレスは、十分に複雑であるか大きいため、推測、推定、または判断することが実現不能または不可能であることを特徴とするシステム。
【請求項１３】
請求項１～１２の何れか１項に記載のシステムにおいて、
前記リンキングアドレスは、ＲＳＩＤ、ＲＣＩＤ、ピン、キー、またはトークンであることを特徴とするシステム。
【請求項１４】
セキュア通信のための方法において、
コンピュータシステムに保存され、それによって実行されるエンジンにおいて、ネットワーク上でデータパケットを第一の電子機器から電子的に受信するステップと、
前記データパケットを処理して、その中に含まれる少なくとも３２ビットのリンキングアドレスとペイロードを特定するステップと、

前記データパケットの前記リンキングアドレスとそれに関連する前記ペイロードを保存するステップと、
第二の電子機器から前記リンキングアドレスを電子的に受信するステップと、
前記データパケットを前記ネットワーク上で前記第二の電子機器に電子的に送信するステップと、
を含むことを特徴とする方法。
【請求項１５】
請求項１４に記載の方法において、
前記リンキングアドレスは少なくとも１２８ビットであることを特徴とする方法。
【請求項１６】
請求項１４～１５の何れか１項に記載の方法において、
前記エンジンは、前記第一の電子機器と前記第二の電子機器の情報を特定することに無関係であることを特徴とする方法。
【請求項１７】
請求項１４～１６の何れか１項に記載の方法において、
前記第一の電子機器と前記第二の電子機器は、前記エンジンが前記データパケットを受信する前に前記リンキングアドレスが一致するように相互にペアリングされることを特徴とする方法。
【請求項１８】
請求項１４～１７の何れか１項に記載の方法において、
前記データパケットを復号するステップをさらに含むことを特徴とする方法。
【請求項１９】
請求項１８に記載の方法において、
復号された前記データパケットの前記ペイロードは暗号化されたペイロードであることを特徴とする方法。
【請求項２０】
請求項１４～１９の何れか１項に記載の方法において、
前記ペイロードは、暗号化されたペイロードであり、前記第二の電子機器に送信される時に暗号化されたままであることを特徴とする方法。
【請求項２１】
請求項１４～２０の何れか１項に記載の方法において、
前記データパケットは役割識別子を含むことを特徴とする方法。
【請求項２２】
請求項１４～２１の何れか１項に記載の方法において、
前記データパケットを前記第二の電子機器に送信する前に前記データパケットを暗号化するステップをさらに含むことを特徴とする方法。
【請求項２３】
請求項１４～２２の何れか１項に記載の方法において、
前記エンジンは、前記第一の電子機器から前記データパケットと共に固有のブラインド証明書を受信することを特徴とする方法。
【請求項２４】
請求項１４～２３の何れか１項に記載の方法において、前記第二の電子機器から前記リンキングアドレスを受信したことに少なくとも部分的に応答して、前記ペイロードを前記第二の電子機器に送信することを判断するステップをさらに含むことを特徴とする方法。
【請求項２５】
請求項１４～２４の何れか１項に記載の方法において、前記リンキングアドレスは、十分に複雑であるか大きいため、推測、推定、または判断することが実現不能または不可能であることを特徴とする方法。
【請求項２６】
請求項１４～２５の何れか１項に記載の方法において、

前記リンキングアドレスは、ＲＳＩＤ、ＲＣＩＤ、ピン、キー、またはトークンであることを特徴とする方法。

【請求項２７】

その上にコンピュータ読取可能命令が保存されている非一時的なコンピュータ読取可能媒体において、コンピュータシステムにより実行された時に、

前記コンピュータシステムに保存され、それによって実行されるエンジンにおいて、ネットワーク上でデータパケットを第一の電子機器から電子的に受信するステップと、

前記データパケットを処理して、その中に含まれる少なくとも３２ビットのリンキングアドレスとペイロードを特定するステップと、

前記データパケットの前記リンキングアドレスとそれに関連する前記ペイロードを保存するステップと、

第二の電子機器から前記リンキングアドレスを電子的に受信するステップと、

前記データパケットをネットワーク上で前記第二の電子機器に電子的に送信するステップと、

を前記コンピュータシステムに実行させることを特徴とするコンピュータ読取可能媒体。

【請求項２８】

請求項２７に記載のコンピュータ読取可能媒体において、

前記リンキングアドレスは少なくとも１２８ビットであることを特徴とするコンピュータ読取可能媒体。

【請求項２９】

請求項２７～２８の何れか１項に記載のコンピュータ読取可能媒体において、

前記エンジンは、前記第一の電子機器と前記第二の電子機器の情報を特定することと無関係であることを特徴とするコンピュータ読取可能媒体。

【請求項３０】

請求項２７～２９の何れか１項に記載のコンピュータ読取可能媒体において、

前記第一の電子機器と前記第二の電子機器は、前記エンジンが前記データパケットを受信する前に前記リンキングアドレスが一致するように相互にペアリングされることを特徴とするコンピュータ読取可能媒体。

【請求項３１】

請求項２７～３０の何れか１項に記載のコンピュータ読取可能媒体において、

前記コンピュータ読取可能命令は、コンピュータシステムにより実行された時に、データパケットを復号するステップを前記コンピュータシステムに実行させることを特徴とするコンピュータ読取可能媒体。

【請求項３２】

請求項３１に記載のコンピュータ読取可能媒体において、

復号された前記データパケットの前記ペイロードは暗号化されたペイロードであることを特徴とするコンピュータ読取可能媒体。

【請求項３３】

請求項２７～３２の何れか１項に記載のコンピュータ読取可能媒体において、

前記ペイロードは、暗号化されたペイロードであり、前記第二の電子機器に送信される時に暗号化されたままであることを特徴とするコンピュータ読取可能媒体。

【請求項３４】

請求項２７～３３の何れか１項に記載のコンピュータ読取可能媒体において、

前記データパケットは役割識別子を含むことを特徴とするコンピュータ読取可能媒体。

【請求項３５】

請求項２７～３４の何れか１項に記載のコンピュータ読取可能媒体において、

前記コンピュータ読取可能命令は、コンピュータシステムにより実行された時に、データパケットを前記第二の電子機器に送信する前にデータパケットを暗号化するステップを前記コンピュータシステムに実行させることを特徴とするコンピュータ読取可能媒体。

【請求項３６】

請求項２７～３５の何れか１項に記載のコンピュータ読取可能媒体において、
前記エンジンは、前記第一の電子機器から前記データパケットと共に固有のブラインド証明書を受信することを特徴とするコンピュータ読取可能媒体。
【請求項３７】
請求項２７～３６の何れか１項に記載のコンピュータ読取可能媒体において、前記コンピュータ読取可能命令は、コンピュータシステムにより実行された時に、前記第二の電子機器から前記リンキングアドレスを受信したことに少なくとも部分的に応答して、前記ペイロードを前記第二の電子機器に送信することを判断するステップを前記コンピュータシステムに実行させることを特徴とするコンピュータ読取可能媒体。
【請求項３８】
請求項２７～３７の何れか１項に記載のコンピュータ読取可能媒体において、前記リンキングアドレスは、十分に複雑であるか大きいため、推測、推定、または判断することが実現不能または不可能であることを特徴とするコンピュータ読取可能媒体。
【請求項３９】
請求項２７～３８の何れか１項に記載のコンピュータ読取可能媒体において、
前記リンキングアドレスは、ＲＳＩＤ、ＲＣＩＤ、ピン、キー、またはトークンであることを特徴とするコンピュータ読取可能媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願との相互参照
本願は、米国特許法第１１９条（ｅ）に基づき、２０１４年６月２日に出願された米国仮特許出願第６１／９９７，４２２号および２０１４年６月２日に出願された米国仮特許出願第６１／９９７，４５０号の利益を主張するものであり、両出願の全体を参照によって本願に援用し、その一部とする。
【０００２】
本願は一般に、リンキングアドレスを用いたネットワーク上でのセキュア通信のためのシステムと方法に関する。より詳しくは、本開示は、多くのリンキングアドレスのうちの１つを用いたネットワーク上でのセキュア送信および保存のためのシステムと方法に関する。
【背景技術】
【０００３】
インターネット上で通信する電子機器の数は増え続けており、これらがまとまって「モノのインターネット（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇｓ）」（ＩｏＴ）をなす。インターネット上でこれほど多くの機器を通信させる難しさから、これらの機器のすべてを相互に直接接続するための効率的で、有効で、信頼性の高い、スケーラブルな方法が提供されている。多くの電子機器は、インターネットに接続する際、ネットワークアドレス変換（Ｎｅｔｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ）（ＮＡＴ）プロトコルを使用する様々なファイヤウォールとルータを介する。ＮＡＴを介した通信では、通信する機器が外部のインターネット環境に直接露出されることはなく、それが露出されたとすれば、その機器が直接通信しようとすると（例えば、機器が、そのインターネットアドレスが露出されているサーバに接続されていないとき）問題となりうる。
【０００４】
Ｉｎｔｅｒｎｅｔ　Ｃｏｎｎｅｃｔｉｖｉｔｙ　Ｅｓｔａｂｌｉｓｈｍｅｎｔ（ＩＣＥ）プロトコル（例えば、Ｓｅｓｓｉｏｎ　Ｔｒａｖｅｒｓａｌ　Ｕｔｉｌｉｔｉｅｓ　ｆｏｒ　ＮＡＴ（ＳＴＵＮ）による）は機器の直接接続を支援するために使用できるが、この方式はすべての場合に機能するわけではない（例えば、全体の１０％）。あるいは、リレイサービスを使用でき（例えば、Ｔｒａｖｅｒｓａｌ　Ｕｓｉｎｇ　Ｒｅｌａｙｓ　ａｒｏｕｎｄ　ＮＡＴ（ＴＵＲＮ））、これはより信頼性が高いが、中継サービスが信頼で

きる当事者である（例えば、その個々のクライアントのほか、ストア許可と接触状態を知っている）必要がある。

【０００５】

これらの方式はサービスのフラグメンテーションをもたらす可能性があり、それは、要求される信頼関係から、機器の各グループ（例えば、ベンダ、プロバイダ、所有者等によりグループ分け）がそれ自体の接続性プロバイダを有するからである。このような方式の別の欠点は、サービス費用の増大であり、これは、信頼性の高い接続がステートフルであるために、サービス側で多くの資源（例えば、処理パワー、メモリ、その他）が必要となるからである。

【０００６】

さらに、多くのシステムと機器は、定期的な、またはイベントドリブンの履歴記録（例えば、ログ）を作成し、これが後の読み出しと解析に備えて保存される。多くの利用可能なログ保存機構は、保存機構とログジェネレータとコンシューマの間が相互に信頼関係にある閉システムを形成する。しかしながら、各システムが独自のログ保存機構を所有しなければならないことは、ログジェネレータとコンシューマが様々な当事者により所有されているとき、誰がそのログコンシューマになるかが不明なとき、複数のログコンシューマがいるとき等に、問題となりうる。さらに、セキュリティアソシエーションと信頼関係をログ保存機構にリンクさせることによって、設定と保持のためのセキュリティアソシエーションと手順の量が増える。すべての解析アプリケーションがそれ自体のログ保存機構を作ること、または製造時に各機器モデルを１つの特定のログ保存機構に限定することは実現困難である。

【０００７】

これらの問題はすべて、ＩｏＴ環境の場合のように、クライアント（例えば、電子機器、機器所有者、その他）の数が増えるとさらに悪化する。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

以上を鑑み、ネットワーク上で、スケーラブルかつ信頼性が高く、最小限のコンピュータ資源と最小限の金銭的資源で設定、保守、および使用できるセキュア電子通信および保存を提供できるシステムが求められている。

【課題を解決するための手段】

【０００９】

本開示は、リンキングアドレスを用いたネットワーク上でのセキュア通信のためのシステムと方法に関する。１つの実施形態において、セキュア通信のためのシステムは、ネットワーク上で複数の電子機器と電子的に通信するコンピュータシステムと、コンピュータシステムと電子的に通信するデータベースであって、少なくともデータパケットのリンキングアドレスおよびそれに関連するペイロードを電子的に保存するように構成されたデータベースと、コンピュータシステムに保存され、それによって実行されるエンジンと、を含み、エンジンは、ネットワーク上で第一の電子機器からデータパケットを電子的に受信し、データパケットを処理して、少なくとも３２ビットであるリンキングアドレスとペイロードを特定し、リンキングアドレスとペイロードをデータベースに保存し、リンキングアドレスを特定する第二の電子機器からのクエリを電子的に受信し、ネットワーク上でデータパケットを第二の電子機器に電子的に送信する。

【００１０】

他の実施形態において、セキュア通信のための方法は、コンピュータシステムに保存され、それによって実行されるエンジンにおいて、ネットワーク上でデータパケットを第一の電子機器から電子的に受信するステップと、データパケットを処理して、その中に含まれる少なくとも３２ビットのリンキングアドレスとペイロードを特定するステップと、データパケットのリンキングアドレスとそれに関連するペイロードをデータベースに保存するステップと、リンキングアドレスを特定する第二の電子機器からクエリを電子的に受信

するステップと、データパケットをネットワーク上で第二の電子機器に電子的に送信するステップと、を含む。

本開示の上記の特徴は、以下の「詳細な説明」を下記のような添付の図面に関連して読むことにより明らかとなるであろう。

【図面の簡単な説明】

【００１１】

【図１】ネットワーク上でのセキュア電子通信および保存のためのＩｏＴ／ＩＰシステムを示す略図である。

【図２】ＩｏＴ／ＩＰエンジンのサブシステムを説明する略図である。

【図３】ＩｏＴ／ＩＰシステムを使用する電子機器の電子的通信を説明する略図である。

【図４】複数の電子機器にまたがるＩｏＴ／ＩＰシステムの使用を説明する略図である。

【図５】ＩｏＴ／ＩＰシステムのセキュア通信中継サブシステムの処理ステップを説明する図である。

【図６】図５の処理ステップを説明する略図である。

【図７】ＩｏＴ／ＩＰシステムのセキュアログ保存サブシステの処理ステップを説明する図である。

【図８】システムのハードウェアおよびソフトウェアコンポーネントを示す略図である。

【発明を実施するための形態】

【００１２】

本開示は、ネットワーク上でのセキュア電子通信および保存のためのシステムと方法に関する。より詳しくは、本開示は、ネットワーク上でのセキュア電子通信および保存を提供するための「モノのインターネット／インターネットプロトコル（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）（ＩｏＴ／ＩＰ）」システムに関する。ＩｏＴ／ＩＰシステムは、スケーラブルかつ信頼性が高く、セキュアであり、最小限のコンピュータ資源（例えば、処理パワー、メモリ、その他）と最小限の金銭的資源で設定、保守、使用できる。使用するコンピュータ資源がより少なくて済むことにより、ＩｏＴ／ＩＰシステムはまた、そのほかの利点の１つとして、コンピュータ自体の機能も改善する。ＩｏＴ／ＩＰシステムは、固有のリンキングアドレス（例えば、キー、ピン、トークン、ＩＤ、その他）を使用することによって、セキュア通信（例えば、電子的送信）およびセキュア保存（例えば、ログ保存）が提供され、このリンキングアドレスは考えうる膨大な数の（例えば、１兆個）リンキングアドレスのうちの１つである。換言すれば、（例えば、電子機器により）使用中のリンキングアドレスの数は、利用可能なリンキングアドレスの数よりはるかに少ない。これによって、使用中のリンキングアドレスを推測または推定することは、コンピュータ化されたランダムアドレスジェネレータを使用したとしても、実現不能（不可能）となる。例えば、リンキングアドレスは３２ビット、６４ビット、１２８ビット、２５６ビット、５１２ビット、その他と大きいか、またはそれより大きくてもよい。ＩＤが１２８ビットである場合、２０兆通りのペアリングの後の衝突確率は１兆分の１であるため、該当するアクティブＩＤを推測または推定する確率は（１兆個のログが同時にアクティブであるとすると）10^{26}分の１である。したがって、ＩｏＴ／ＩＰシステムは、いかなるセキュリティアソシエーションも必要とせず、または使用しない。

【００１３】

図１は、概して１０で示される、ネットワーク上でのセキュア通信および保存のためのある例示的なＩｏＴ／ＩＰシステムを示す略図である。ＩｏＴ／ＩＰシステム１０は、その中に保存された、またはそこに動作的に接続されたデータベース１４を有するコンピュータシステム１２（例えば、１つのサーバ、複数のサーバ）と、ＩｏＴ／ＩＰエンジン１６と、を含む。コンピュータシステム１２は、何れの適当なオペレーティングシステム（例えば、ＭｉｃｒｏｓｏｆｔによるＷｉｎｄｏｗｓ、Ｌｉｎｕｘ、その他）を実行する何れの適当なコンピュータサーバ（例えば、ＩＮＴＥＬマイクロプロセッサ、複数のプロセッサ、複数の処理コア、その他を搭載したサーバ）であってもよい。データベース１４は

、コンピュータシステム１２上に保存されても、またはその外部に（例えば、ＩｏＴ／ＩＰシステム１０と通信する別のデータベースサーバの中に）あってもよい。ＩｏＴ／ＩＰシステム１０は遠隔的にアクセス可能であり、それによってＩｏＴ／ＩＰシステム１０はネットワーク２０を通じて様々なコンピュータシステム２２（例えば、パーソナルコンピュータシステム２６ａ、スマート携帯電話２６ｂ、タブレットコンピュータ２６ｃ、および／またはその他の電子機器）のうちの１つまたは複数と通信する。ネットワーク通信はインターネット上で、標準ＴＣＰ／ＩＰ通信プロトコル（例えば、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、セキュアＨＴＴＰ（ＨＴＴＰＳ）、ファイル転送プロトコル（ＦＴＰ）、電子データ交換（ＥＤＩ）、その他）を使って、プライベートネットワーク接続（例えば、ｗｉｄｅ－ａｒｅａ　ｎｅｔｗｏｒｋ（ＷＡＮ）接続、電子メール、電子データ交換（ＥＤＩ）メッセージ、Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ（ＸＭＬ）メッセージ、ファイル転送プロトコル（ＦＴＰ）ファイル転送その他）、またはその他のあらゆる適当な有線またはワイヤレス電子通信フォーマットおよびシステムを通じて行われてもよい。

【００１４】

図２は、ＩｏＴ／ＩＰエンジン１６の例示的なサブシステムを説明する略図である。これらは、セキュア通信中継サブシステム３０と、セキュアログ保存サブシステム３２と、を含む。セキュア通信中継サブシステム３０は、固有のリンキングアドレス（例えば、事前に同意されたもの）を利用することにより、ネットワーク上で２つ（またはそれ以上の）電子機器間のセキュア通信の匿名中継を（例えば、リアルタイムで）提供する。より詳しくは、セキュア通信中継サブシステム３０のためのリンキングアドレスは、Ｒｅｍｏｔｅ　Ｃｏｎｄｕｉｔ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ（ＲＣＩＤ）であってもよい。前述のように、所定のＲＣＩＤは非常に複雑であり（例えば、大きく）、推測や判断が実現不能であり、利用可能な固有のＲＣＩＤの数は、使用中の実際の数よりはるかに大きい。セキュア通信中継サブシステム３０は、電子機器の識別と送信されるデータパケット（例えば、電子通信）の内容とは全く無関係（例えば、非依存的）である。

【００１５】

セキュアログ保存サブシステム３２は、第一のログジェネレータ電子機器から生成されるログエントリ（または他の何れかの種類のデータ）の匿名保存を提供し、すると、これには１つまたは複数の第二のログコンシューマ電子機器がリンキングアドレスを使用することによりアクセスできる。第一のログコンシューマ電子機器は、第二のログジェネレータ電子機器と同じ機器であってもよい。より具体的には、セキュアログ保存サブシステム３２のためのリンキングアドレスは、Ｒｅｍｏｔｅ　Ｓｔｏｒａｇｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ（ＲＳＩＤ）であってもよい。ログジェネレータ電子機器は、ログエントリを１つのＲＳＩＤに送信してもよく、すると、これには１つまたは複数のログコンシューマ電子機器がアクセスできる。あるいは、ログジェネレータ電子機器は、ログエントリを複数のＲＳＩＤに送信してもよく、それによって各リンキングアドレスは１つのログコンシューマ電子機器に専用となる。セキュア通信中継サブシステム３０と同様に、ＲＳＩＤは非常に複雑で（例えば、大きく）、使用中のアドレスを推測または推定するのは実現不能であり、利用可能な固有のＲＳＩＤの数は、使用中の実際の数よりはるかに多い。セキュアログ保存サブシステム３２は、電子機器の識別と、送信され、保存されるデータパケット（例えば、ログエントリ）の内容とは完全に無関係（例えば、非依存的）である。ログエントリが説明されているが、セキュアログ保存サブシステム３２は何れの種類の電子データを保存してもよい。

【００１６】

ＩｏＴ／ＩＰシステムは、いかなる機密情報またはクライアント情報（例えば、登録情報、コンフィギュレーション情報、ハードウェアアドレス情報、その他）も保存せず、それゆえ、ＩｏＴ／ＩＰシステムのサーバは保護の必要がない。換言すれば、ＩｏＴ／ＩＰシステム（例えば、セキュア通信中継サブシステム３０とセキュアログ保存サブシステム３２の各々を含む）には、それと通信している電子機器もわからなければ、ＩｏＴ／ＩＰ

システムには、そのような機器のセキュリティアソシエーションもわからない。その結果、ＩｏＴ／ＩＰシステムは、非常に少額な金銭的費用で動作し、最小限のコンピュータ資源しか使用しないため、コンピュータ自体の機能（例えば、速度）が改善される。ＩｏＴ／ＩＰシステムは、電子機器の何れに関する情報や知識も、それらの機器がそのシステムを使用する前に必要としないため、コストのかかる認証システムや手順（例えば、ログイン、アカウント、その他）を回避できる。これは多数の機器（例えば、数百万の機器）間の相互接続性インフラストラクチャを提供し、準備ステップは一切不要であり、個々の機器の情報の通信も不要である。

【００１７】

図３は、ＩｏＴ／ＩＰシステムを使った電子機器の電子通信の一例を説明する略図である。より詳しくは、第一の電子機器（例えば、スマートランプ４０）は第二の電子機器（例えば、スマートフォン４２）と、これら２つの機器を安全にペアリングする（例えば、２つの機器をローカルで認証する）ためのローカル通信スタック３４を使ってローカルで通信する（例えば、Ｂｌｕｅｔｏｏｔｈ、Ｂｌｕｅｔｏｏｔｈ　Ｌｏｗ　Ｅｎｅｒｇｙ、Ｗｉ－Ｆｉ）。このように安全にペアリングする間に、２つの電子機器は１つまたは複数の固有のリンキングアドレス（例えば、ＲＣＩＤおよび／またはＲＳＩＤ）について一致する。しかしながら、これらの機器は他の様々な代替的方法の何れによっても安全にペアリングされてよい（例えば、製造者が事前設定する）。リンキングアドレスが一致したら、２つの電子機器（例えば、スマートランプ４０とスマートフォン４２）は、このリンキングアドレスを使ってインターネット上で相互にリモートで通信できる。より詳しくは、スマートランプ４０は、データパケット（例えば、通信）をセキュア通信中継サブシステム３０の所定のＲＣＩＤに送信できる（例えば、Ｃｏｎｄｕｉｔ　ＩｏＴ／ＩＰサービス）。すると、スマートフォン４２はＲＣＩＤを使ってこのデータパケットをセキュア通信中継サブシステム３０から読み出すことができる（例えば、リアルタイムアラートのため）。スマートランプ４０はまた、データパケット（例えば、ログエントリ）をセキュアログ保存サブシステム３２のＲＳＩＤに送る（例えば、ストリーミング）することができ（例えば、ＥＳｒｔｏｒａｇｅ　ＩｏＴ／ＩＰサービス）、これはそのデータパケットをそのＲＳＩＤに、後に例えばある電子機器のアプリケーションプログラミングインタフェース（ＡＰＩ）４４によって読み出されるまで保存する。図３の例は、ワイヤレス通信システムであるように示されているが、ワイヤレスでも有線でも、何れの適当な通信システムが使用されてもよい。

【００１８】

図４は、複数の電子機器をまたぐＩｏＴ／ＩＰシステムのある例示的な使用を説明する略図である。図のように、前述の通りに、第一の電子機器（例えば、スマートランプ４０）は１つまたは複数の第二の電子機器（例えば、ローカルスマートフォン４２ａ、ローカルルータ４６、その他）とローカルで通信する（例えば、Ｂｌｕｅｔｏｏｔｈ、Ｂｌｕｅｔｏｏｔｈ　Ｌｏｗ　Ｅｎｅｒｇｙ、Ｗｉ－Ｆｉ、その他を使用）。より詳しくは、例えば、スマートランプ４０は、第一の（有線またはワイヤレス）通信リンク４５ａでスマートフォン４２ａとローカルで通信してもよく（例えば、ＲＣＩＤについて一致するため）、スマートランプ４０はまた、第二の（有線またはワイヤレス）通信リンク４５ｂでルータ４６と通信してもよく、スマートフォン４２ａは、第三の（有線またはワイヤレス）通信リンク４５ｃで通信してもよい。したがって、スマートランプ４０、スマートフォン４２ａ、およびルータ４６は、相互に信頼できる機器として認証される。

【００１９】

ローカルで認証されると、これらの機器はＩｏＴ／ＩＰシステムを介してインターネット２０上で遠隔的に相互に直接通信できる。例えば、リモートスマートフォン４２ｂ（異なっていても、離れた場所にあるときにスマートフォン４２と同じスマートフォンであってもよい）はＩｏＴ／ＩＰエンジン１６と通信してもよく、これがローカルルータ４６を介してスマートランプ４０と通信する。システムは、使用されるローカル電子通信プロトコルと完全に無関係である（例えば、ＮＡＴプロトコルと無関係）。何れの数の、または

何れの種類の電子機器でも使用され、相互にペアリングされて（例えば、スマートランプ４０、デスクトップコンピュータ４８、スマートフォン５０、タブレットコンピュータ５２、ラップトップコンピュータ、サーモスタット、ＬｉｇｈｔＳｗｉｔｃｈ、電気ソケット、ガレージドアオープナ、その他）、ＩｏＴ／ＩＰエンジン１６を介して相互にリモートで通信してもよい。ユーザの観点から、機器（例えば、スマートランプ４０とスマートフォン４２ａ）は、相互にローカルで通信し（例えば、Ｂｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、その他を使用）、一致するリンキングアドレスを決定し、その後、決定されたリンキングアドレスを使って、ネットワーク２０上で相互にリモートで通信してもよい（例えば、スマートランプ４０とスマートフォン４２ｂ）。ユーザの観点から、機器は、ローカルで通信する際に、リモートで通信するときと同様に、（例えば、ユーザ、機器のハードウェア、および／または他の何れかの識別情報の）オンライン登録を必要とせずに相互に通信し、動作する。さらに、システムは前方秘匿性を利用してもよく、それによって、認証されない使用者が機器および／またはＩｏＴ／ＩＰシステムに侵入した時に過去の通信を再構築できない。

【００２０】

図５は、ある例示的なＩｏＴ／ＩＰシステムのセキュア通信中継サブシステムの処理ステップ６０を示す。ステップ６２で、ＩｏＴ／ＩＰシステムはネットワーク上で、第二の電子機器（例えば、機器Ｂ、機器２、その他）とペアリングされた（例えば、同期された、認証された）第一の電子機器（例えば、機器Ａ、機器１、その他）からデータパケット（例えば、パケット、メッセージ、通信、記録、その他）を受信する。第一の電子機器と第二の電子機器はペアリングされ、これらの機器はＲｅｍｏｔｅ Ｃｏｎｄｕｉｔ Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ（ＲＣＩＤ）（例えば、リンキングアドレス）と、両者間を区別する（例えば、ＡかＢか、１か２か、その他）ための役割識別子（例えば、役割）で一致する。ＲＣＩＤは、様々な実施形態において、非常にスパースなネームスペースの中に存在し、ランダムトークン、番号、単語、パスフレーズ、記号、その他とすることができる。十分な複雑さの（例えば、サイズ、可変性、その他）ＲＣＩＤが使用された場合、利用されている特定のＲＣＩＤを推測または推定することは実現不能である。例えば、ＲＣＩＤは１２８ビットのトークンであってもよい。２つの電子機器は、様々な適当な方法のうちの何れによっても相互にペアリングできる（例えば、共通のＲＣＩＤで一致する）。例えば、２つの電子機器は、相互に直接通信することも（例えば、Ｂｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、その他を使用）、２つの電子機器は、製造者によりそれらの機器が共通のＲＣＩＤで事前にプログラムされているように、パッケージ化して販売することも、および／または２つの電子機器は、２つの機器を相互に同期させるウェブサイトに登録することもできる。あるいは、ユーザはＲＣＩＤを機器の各々に手で入力し、および／またはＲＣＩＤと相関させるための事前にプログラムされた数学的アルゴズムにより処理される固有のパスフレーズ（例えば、単語、文、その他）を手で入力することができる（例えば、各機器へのパスフレーズの入力は、同じアルゴリズムにより処理され、各機器が独立して同じＲＣＩＤに到達する）。２つの電子機器はまた、セキュアでないチャネル上でのセキュア通信を可能にする、確立された認証情報（例えば、共有の秘密）を有していてもよい。より詳しくは、このように確立された認証情報によって、機器間でのエンドツーエンド暗号化が可能となり、ＩｏＴ／ＩＰシステムおよび／または他の誰かからの通信を保護できる。ステップ６４で、ＩｏＴ／ＩＰシステムは、データパケットがＩｏＴ／ＩＰシステムのサーバの公開キーにより暗号化されていれば、それを復号する。データパケット暗号化は、ＲＣＩＤを観察者から隠し、第三者による干渉を防止する（例えば、第三者がそのＲＣＩＤを知るのを防ぐ）。データパケットを暗号化するために、既存の公開キー方式の何れを使用してもよい（例えば、ＲＳＡ、ディフィ・ヘルマン（ＤＨ）、楕円曲線暗号（ＥＣＣ）、その他）。しかしながら、前述のように、ＩｏＴ／ＩＰシステムはセキュリティアソシエーションを必要としない。特に、エンドツーエンド暗号化が行われるデータパケットと事前に確立された認証情報による認証の場合、クライアントとＩｏＴ／ＩＰシステムとの間の電子通信（例えば、トラフィック）のセキュリティを確保する必要はない。Ｉ

ｏＴ／ＩＰサーバの公開キーでのＲＣＩＤの暗号化とスパースなＩＤネームスペースの使用によって、攻撃者は悪意あるトラフィックまたはログエントリを挿入したり、または正当なユーザになりすましたりすることができず、それによって標的を絞ったサービス妨害攻撃と覗き見が防止される。ステップ６６で、ＩｏＴ／ＩＰシステムは次に、受信したデータパケットを処理して、ＲＣＩＤ、役割識別子（例えば、ＡかＢか、１か２か、その他）、およびペイロード（例えば、暗号化されたペイロード）を特定する。ステップ６８で、ＩｏＴ／ＩＰシステムは、第一の役割がアクティブか否かを判断する。各電子機器（例えば、第一の電子機器と第二の電子機器）は、（例えば、データパケットを電子的に送信する前または送信中に）例えばＩｏＴ／ＩＰシステムに開チャネルリクエストを電子的に送信すること等により、ＩｏＴ／ＩＰシステム（例えば、サーバ）でＲＣＩＤの役割のアクティブ状態を確立できる。開チャネルリクエストは、ＩｏＴ／ＩＰシステムで有効性確認して、その電子機器がそのＩｏＴ／ＩＰシステムを使用する権限を有することを確認するためのＲＣＩＤ、役割、および／または認証情報（例えば、固有のブラインド証明書を含むことができる。ＩｏＴ／ＩＰシステムが開チャネルリクエスト（例えば、認証情報を含む）の有効性を確認すると、ＩｏＴ／ＩＰシステムはＲＣＩＤの役割（例えば、第一の役割）の状態がアクティブであると宣言する。電子機器がＲＣＩＤの役割のアクティブ状態を確立すると、ＩｏＴ／ＩＰシステムは、開チャネルリクエストの受信時間を記録し、タイマをスタートさせることができる。所定の時間が経過すると（例えば、２分、５分、その他）、ＩｏＴ／ＩＰシステムは、電子機器がアクティブ状態のままでないかぎり、アクティブ状態を解除する（例えば、役割の状態をイナクティブに変更する）。電子機器は、開チャネルリクエストを（例えば、認証情報と共に）再送信するか、または後述のように第二の電子機器へのデータパケットの送信を成功させることによって、アクティブ状態を保持し、タイマをリセットすることができる。第一の役割がアクティブでない（例えば、イナクティブである）場合、システムはステップ７６に進み、データパケットをドロップする。第一の役割がアクティブで場合、ステップ７０で、ＩｏＴ／ＩＰシステムはそのデータパケットのＩＰアドレスおよび／または受信時間をデータベースに記録する。ステップ７２で、ＩｏＴ／ＩＰシステムは、第二の役割（例えば、第二の電子機器）がアクティブであるか否かを判断する。アクティブであれば、ステップ７４で、ＩｏＴ／ＩＰシステムはデータパケットを（暗号化されたペイロードとともに）第二の電子機器に送る。ＩｏＴ／ＩＰシステムは、いくつかの実施形態において、第二の電子機器に送信するためにデータパケットを暗号化する。第二の役割がアクティブでない場合、ステップ７６で、システムはデータパケットをドロップする。受信時に、第二の電子機器は暗号化されたパケット（暗号化されている場合）と暗号化されたペイロード（暗号化されている場合）の両方を復号できる。このようにして、ＩｏＴ／ＩＰシステムは、第一の電子機器と第二の電子機器との間の中継点として機能する。ＩｏＴ／ＩＰシステムは、電子機器の識別、暗号化されたペイロードの内容、電子機器の一方または両方の所有者の識別、その他と完全に無関係（例えば、非依存的）である。しかしながら、ＲＣＩＤが非常に大きいため、ＩｏＴ／ＩＰはネットワーク上での電子通信に必要なプライバシとセキュリティを提供する。

【００２１】

図６は、図５の例示的な処理ステップを説明する略図である。より詳しくは、図のように、クライアントＡ　８０（例えば、第一の電子機器）とクライアントＢ　８２はがセキュアにペアリングされており、これらは事前設定されたＲＣＩＤ　８４で一致している。クライアントＡ　８０はすると、クライアントＢ　８２のためのデータパケット８８をネットワーク上で中継点８６（例えば、ＩｏＴ／ＩＰシステム）に送信する。データパケット８８にはＲＣＩＤ　９０（例えば、事前設定されたＲＣＩＤ　８４と同じ）、送信するクライアントの役割識別子９２（例えば、クライアントＡ　８０から送信される場合はＡ、クライアントＢ　８２から送信される場合はＢ）、および暗号化されたペイロード９４が含まれるが、前述のように、他の実施形態において、ペイロードは暗号化されていない。中継点８６は、クライアントＡ　８０からデータパケット８８を受信し、次にデータパケット８８を復号してＲＣＩＤ　９０、役割識別子８２、および暗号化されたままのペイ

ロード９４（ペイロードが暗号化されていない場合、このステップは、行われない）を明らかにする。クライアントＢ　８２は事前設定されたＲＣＩＤ　８４を使って中継点８６からのデータパケット８８を読み出し、その後、データパケット８８と暗号化されたペイロード９４を復号する。中継点８６は、いくつかの実施形態において、クライアントＢ８２に送信するためにデータパケット８８を暗号化する。いくつかのこのような実施形態において、データパケット８８の中の復号化されたペイロード９４は、中継点８６によって復号されない。中継点８６は、ペイロードの復号ではなく、データパケットの復号のみを提供する。

【００２２】

図７は、例示的なＩｏＴ／ＩＰシステムのセキュアログ保存サブシステムの処理ステップ１００を説明する。ステップ１０２で、ＩｏＴ／ＩＰシステムはネットワーク上でデータパケット（例えば、メッセージ、通信、記録、その他）を１つまたは複数のログコンシューマ（例えば、第二の電子機器）とペアリングされた（例えば、同期された）ログジェネレータ（例えば、第一の電子機器）から受信する。ログジェネレータとログコンシューマはペアリングされ、それによってこれらの機器はＲｅｍｏｔｅ　Ｓｔｏｒａｇｅ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ（ＲＳＩＤ）（例えば、リンキングアドレス）で一致する。各種の実施形態において、ＲＳＩＤは非常にスパースなネームスペースにあり、ランダムトークン、番号、単語、パスフレーズ、記号、その他とすることができる。ＲＳＩＤが十分に複雑なもの（例えば、大きさ、可変性、その他）であるべきである場合、使用されているその特定のＲＳＩＤの推測または推定は実現不能である。例えば、ＲＳＩＤは１２８ビットのトークンであってもよい。ログジェネータとログコンシューマ（例えば、２つの電子機器）は、様々な方法のうちの何れで相互にペアリングされてもよい（例えば、そして共通のＲＳＩＤで一致する）。例えば、２つの電子機器は、相互に直接通信することも（例えば、Ｂｌｕｅｔｏｏｔｈ、Ｗｉ－Ｆｉ、その他を使用）、２つの電子機器は、製造者によりそれらの機器が共通のＲＣＩＤで事前にプログラムされているように、パッケージ化して販売することも、および／または２つの電子機器は、２つの機器を相互に同期させるウェブサイトに登録することもできる。あるいは、ユーザはＲＣＩＤを機器の各々に手で入力し、および／またはＲＣＩＤと相関させるための事前にプログラムされた数学的アルゴズムにより処理される固有のパスフレーズ（例えば、単語、文、その他）を手で入力することができる（例えば、各機器へのパスフレーズの入力は、同じアルゴリズムにより処理され、各機器が独立して同じＲＣＩＤに到達する）。それに加えて、またはその代わりに、ログジェネレータはＲＳＩＤを前もって作り、それを使ってログエントリを保存し、その後、このＲＳＩＤを１つまたは複数のログコンシューマに電子的に通信することもできる。セキュアソケットレイヤ（ＳＳＬ）、その他等、何れの適当な電子通信方法が使用されてもよい。２つの電子機器はまた、確率された認証情報（例えば、共有の秘密）を有していてもよく、これによってセキュアでないチャネル上でのセキュア通信が可能となる。より詳しくは、このような確立された認証情報により、機器間のエンドツーエンド暗号化が可能となり、ＩｏＴ／ＩＰシステおよび／またはその他の誰かからの通信が保護される。このようにして、データパケット全体が、ＲＳＩＤを有する第一の暗号化によって暗号化され、ペイロードは第二の暗号化により暗号化されてもよい。それゆえ、ログエントリは、暗号化された状態で保存でき、権限を有するログコンシューマだけがこれらを復号できる。ステップ１０４で、ＩｏＴ／ＩＰシステムは、受信したデータパケットがＩｏＴ／ＩＰシステムのサーバの公開キーで暗号化されていれば、復号する。データパケットの暗号化により、ＲＳＩＤが観察者から隠され、第三者による干渉が防止される（例えば、第三者がＲＳＩＤを知るのを防止する）。データバケットを暗号化するには、既存の公開キー方式の何れでも使用できる（例えば、ＲＳＡ、ディフィーホルマン（ＤＨ）、楕円曲線暗号化（ＥＣＣ）その他）。しかしながら、前述のように、ＩｏＴ／ＩＰシステムはセキュリティアソシエーションを必要としない。ログジェネレータおよび／またはログコンシューマからＩｏＴ／ＩＰシステムへの電子通信は、ＩｏＴ／ＩＰシステムのサーバの公開キーで暗号化できる。ステップ１０６で、ＩｏＴ／ＩＰシステムは次に、受信したデ

ータパケットを処理して、ＲＳＩＤとペイロード（例えば、暗号化されたペイロード）を特定し、それによってログエントリをＲＳＩＤに関連付ける。ステップ１０８で、ＩｏＴ／ＩＰシステムはデータパケットのＩＰアドレスおよび／または受信時間（例えば、データパケットにタイムスタンプを追加）をデータベースに記録する。ステップ１１０で、ＩｏＴ／ＩＰシステムはパケットをデータベース（例えば、キー値データベース）に保存する。例えばＲｉａｋ等、様々なデータベースの何れでも使用できる。保存機構は、少なくともＲＳＩＤのみに基づく読み出し動作を提供する。これに加えて、保存機構はまた、ＲＳＩＤとタイムスタンプ範囲に基づく読み出し、ＲＳＩＤに関連するコンテンツの削除、および／またサイレントログ記録のドロップ（例えば、ＲＳＩＤごとの経過年数および／または能力に到達したか、これを超えた後）を提供してもよい。ペイロードが暗号化されている場合、保存情報を保護するための様々な手順のうちの何れでも使用できる。例えば、暗号化されたペイロードは、ランダムｓａｌｔ（例えば、初期化ベクタ（Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒ）（ＩＶ）、その他）、ペイロード長さ、および／またはログエントリによる初期化ベクタ（例えば、共有の秘密をキーとして使用したストリーム暗号による暗号化）を含むことができる。

【００２３】

ステップ１１２で、ＩｏＴ／ＩＰシステムはログコンシューマからクエリ（例えば、リクエスト）を受信する。リクエストは、ＲＳＩＤを含み、任意選択でクエリ用語（例えば、読み出される最新のエントリの最大数および／または読み出すべき最も古いエントリの時間、その他）を含んでいてもよい。リクエストは、ＩｏＴ／ＩＰシステムのサーバの公開キーで暗号化されてもよい。この暗号化により、ＲＳＩＤが観察者から隠され、第三者による干渉が防止される（例えば、第三者がＲＳＩＤを知るのを防止する）。データパケットを暗号化するために、既存の公開キー方式の何れでも使用できる（例えば、ＲＳＡ、ディフィーヘルマン（ＤＨ）、楕円曲線暗号化（ＣＤＤ）、その他）。しかしながら、前述のように、ＩｏＴ／ＩＰシステムはセキュリティアソシエーションを必要としない。特にエンドツーエンド暗号化によるデータパケットと事前に確立された認証情報による認証に関して、クライアントとＩｏＴ／ＩＰシステムとの間の電子通信（例えば、トラフィック）のセキュリティを確保する必要はない。ＩｏＴ／ＩＰサーバの公開キーでのＲＳＩＤの暗号化とスパースなＩＤネームスペースを使用することによって、攻撃者は悪意あるトラフィックまたはログエントリを挿入したり、正当な通信ピアまたはコンシューマになりすましたりすることができず、それによって標的を絞ったサービス拒否（ｄｅｎｉａｌ　ｏｆ　ｓｅｒｖｉｃｅ）（ＤｏＳ）の攻撃と覗き見を防止できる。ステップ１１４で、ＩｏＴ／ＩＰシステムは要求されたログエントリ（例えば、クエリ用語と一致するもの）をデータベースから読み出す。ステップ１１６で、ＩｏＴ／ＩＰシステムはログエントリをログコンシューマに電子的に送信する。暗号化されている場合、ログエントリ（例えば、ペイロード）は第三者には不透明なままである。電子通信は、タイムスタンプを含み、および／または、例えばＩｏＴ／ＩＰシステムサーバとログコンシューマによって暗号化されてもよく、それによって公開キー方式（例えば、ディフィーヘルマン）による１回の共有秘密が確立される。このようにして、ＩｏＴ／ＩＰシステムは、第一の電子機器と第二の電子機器との間のストレージとして機能する。ＩｏＴ／ＩＰシステムは、電子機器（例えば、ログジェネレータ、ログコンシューマ、その他）の識別、暗号化されたログエントリの内容、電子機器の一方または両方の所有者の識別、その他と完全に無関係（例えば、非依存的）である。しかしながら、ＲＳＩＤ範囲は非常に大きいため、一致した当事者（例えば、ログジェネレータとログコンシューマ）しかログエントリを保存し、読み出しすることができない。これによって、ＩｏＴ／ＩＰは、ネットワーク上の電子通信に必要なプライバシとセキュリティを提供する。ＩｏＴ／ＩＰシステム（例えば、セキュア中継通信サブシステム、セキュアログ保存サブシステム）は、クライアント（例えば、電子機器、電子機器の所有者、その他）に関する識別情報は一切処理または保存しない。これによって設定費用、保守費用、およびデータ保存要求が大幅に減少する。しかしながら、ＩｏＴ／ＩＰシステムはいかなる識別情報も使用しないため、無関係な当事者（例えば、不正な

ユーザ）がＩｏＴ／ＩＰシステムの使用を試みることはできない。したがって、希望に応じて、不正使用や無許可の使用者（例えば、支払を行っていないユーザ）による使用に対抗するために、認証された電子機器の各々には、固有のブラインド証明書を発行できる。固有のブラインド証明書（例えば、官公庁の文書）を定期的に（例えば、最初のログエントリと共に、毎回のイナクティブタイマ時間ごとに、その他）提出を求めることができる。固有のブラインド証明書は、製造者により埋め込まれても、オンライン登録から発行されても、その他であってもよい。それゆえ、ＩｏＴ／ＩＰシステムは、有効な証明書を認識できるが、それを特定の電子機器および／またはユーザに関連付けない。ＩｏＴ／ＩＰシステムは、いくつかの実施形態において、不正使用の兆候をモニタしてもよく、不正使用の原因となったことが判明した証明書および／またはＩＰアドレスのすべてをブラックリストに入れ（例えば禁止し）、それによってそのＩＰアドレスまたは証明書の保有者がＩｏＴ／ＩＰシステムにアクセスするのを防止することができる。このような不正使用の兆候としては、ＩＰアドレスが頻繁に変更されすぎるような、あるＩＰアドレスによる特定のＲＣＩＤへのアクセス、同じ証明書を有するが、異なるＩＰアドレスの２つの機器による特定のＲＳＩＤの同時使用、または第三の電子機器による特定のＲＣＩＤの使用の試み、その他を含むことができる。

【００２４】

スパースなＩＤ（例えば、リンキングアドレス、ＲＳＩＤ、ＲＣＩＤ）ネームスペースを使用することによって、クライアントサイドの負荷バランスは非常に効率的となり、高い有用性が提供される。Ｎ個のログサーバ（接続されていなくてもよい）を想定すると、各クライアント（例えば、ジェネレータ、コンシューマ、クライアントＡ、クライアントＢ、その他）は、すべてのアクティブサーバ（例えば、Ｓｅｒｖｅｒ［Ｎ］）のアドレスリストを有する。あるサーバを選択するには、クライアント（例えば、ジェネレータ、コンシューマ、クライアントＡ、クライアントＢ、その他）がインデックスｉ＝ＩＤｍｏｄＮ（式中、ＩＤはＲＣＩＤまたはＩＳＤＩの何れか）を計算し、両方がＳｅｒｖｅｒ［ｉ］を選択する。少なくともＩＤがランダムに選択される実施形態では、負荷はＮ個のログサーバで均等に分散され、追加の手順は不要である。ＩＤを直接使用する代わりに、ＩＤのハッシュ（例えば、ｉ＝ｈａｓｈ（ＩＤ）ｍｏｄ　Ｎ）を使って、ＩＤのランダム性が低い場合の影響を回避してもよい。

【００２５】

ＩＤのハッシュの使用はまた、不具合のあるログサーバを回避するためにも利用できる。例えば、あるログサーバが特定のパケットに想定通りに応答しない（例えば、応答が到達しない）場合、ジェネレータまたはコンシューマはＲＳＩＤを単に１つ進め、新しいｉ＝ｈａｓｈ（ＲＳＩＤ）ｍｏｄＮを再び計算し、サーバが応答するまでこれを続ける。

【００２６】

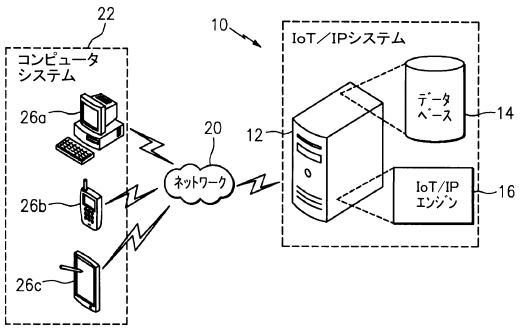
図８は、ある例示的なＩｏＴ／ＩＰシステム２００ハードウェアおよびソフトウェアコンポーネントを示す略図である。システム２００は処理サーバ２０２を含み、これは記憶装置２０４、ネットワークインタフェース２０８、通信バス２１０、中央処理ユニット（ＣＰＵ）（マイクロプロセッサ）２１２、ランダムアクセスメモリ（ＲＡＭ）２１５、およびキーボード、マウス等の１つまたは複数の入力装置２１６のうちの１つまた複数を含んでいてもよい。サーバ２０２はまた、ディスプレイ（例えば、液晶ディスプレイ（ＬＣＤ）、陰極管（ＣＲＴ）、その他）も含んでいてよい。記憶装置２０４は、何れの適当なコンピュータ読取可能記憶媒体、例えばディスク、不揮発性メモリ（例えば、リードオンリメモリ（ＲＯＭ）、イレーサブルプログラマブルＲＯＭ（ＥＰＲＯＭ）、エレクトリカリイレーサブルプログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、その他）を含んでいてもよい。サーバ２０２は、ネットワーク化されたコンピュータシステム、パーソナルコンピュータ、スマートフォン、タブレットコンピュータ、その他であってもよい。本開示により提供される機能性は、ＩｏＴＩＰプログラム／エンジン２０６によって提供されてもよく、これは記憶装置２０４に保存され、ＣＰＵ　２１２によって何れかの適当なハイレベルまたはローレベル

コンピュータ言語、例えばＰｙｔｈｏｎ、Ｊａｖａ、Ｃ、Ｃ＋＋、Ｃ＃、．ＮＥＴ、ＭＡＴＬＡＢ、その他を使って実行されるコンピュータ読取可能プログラムコードとして具現化されてもよい。ネットワークインタフェース２０８は、イーサネットネットワークインタフェースデバイス、ワイヤレスネットワークインタフェースデバイス、または、サーバ２０２がネットワークを介して通信できるようにする、他の何れの適当なデバイスを含んでいてもよい。ＣＰＵ　２１２は、ＩｏＴ／ＩＰエンジン２０６を実装し、実行可能な何れの適当なアーキテクチャの何れの適当なシングルまたはマルチコアマイクロプロセッサ（例えば、Ｉｎｔｅｌプロセッサ）を含んでいてもよい。ランダムアクセスメモリ２１４は、ダイナミックＲＡＭ（ＤＲＡＭ）その他、最も現代的なコンピュータに典型的な何れの適当な高速ランダムアクセスメモリを含んでいてもよい。

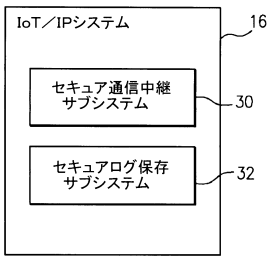
【００２７】

以上、システムと方法を詳しく説明したが、上記の説明は本発明の主旨または範囲を限定しようとするものではないと理解すべきである。当然のことながら、本明細書に記載されている本開示の実施形態は例にすぎず、当業者は、本開示の主旨と範囲から逸脱することなく、何れの変更および改良を加えることもできる。かかる変更と改良はすべて、上述のものを含め、本開示の範囲内に含められるものとする。

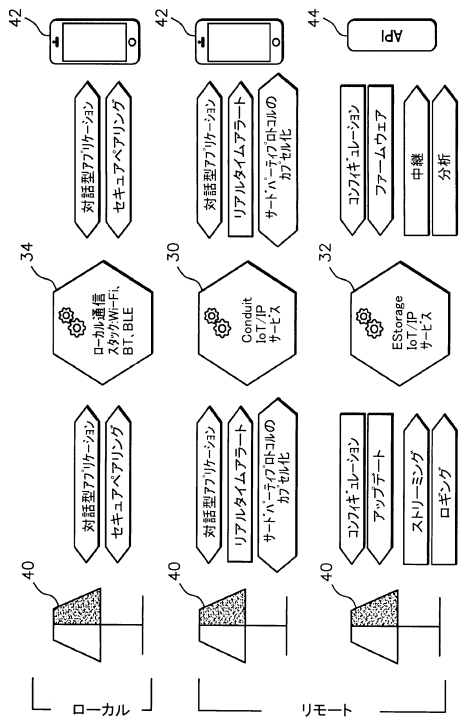
【図１】



【図２】



【図３】



【図４】

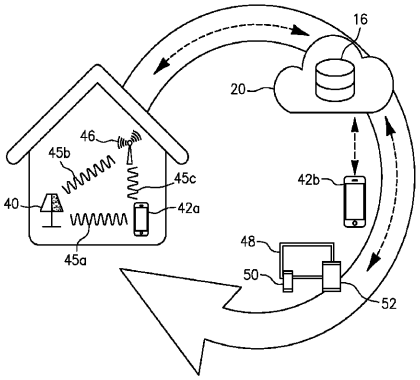
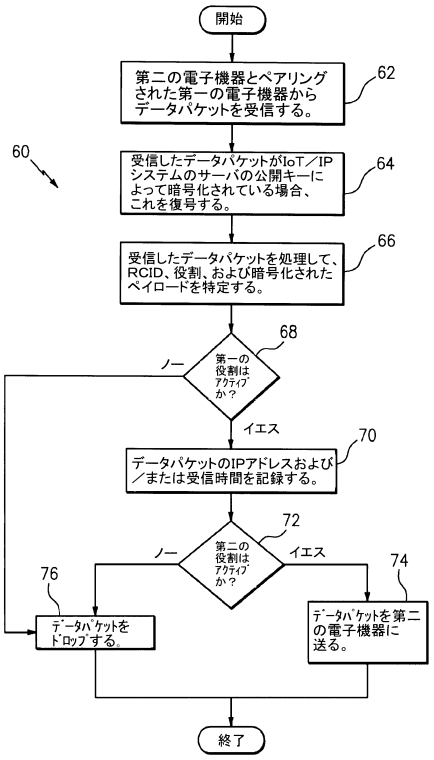
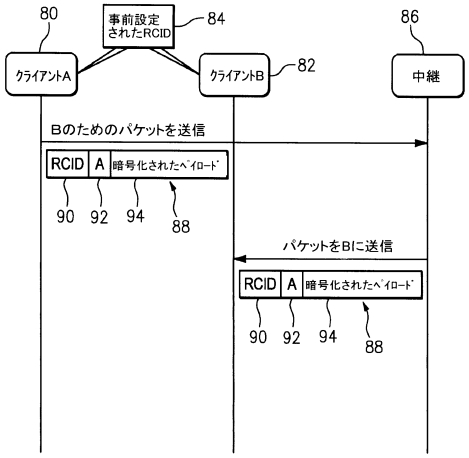


FIG. 4

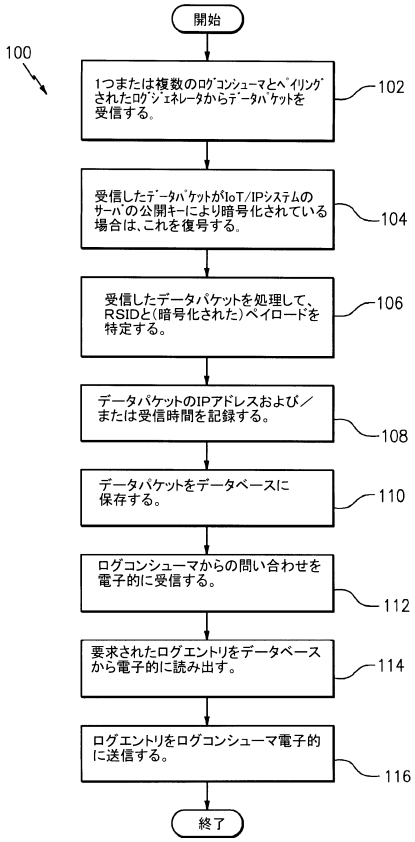
【図５】



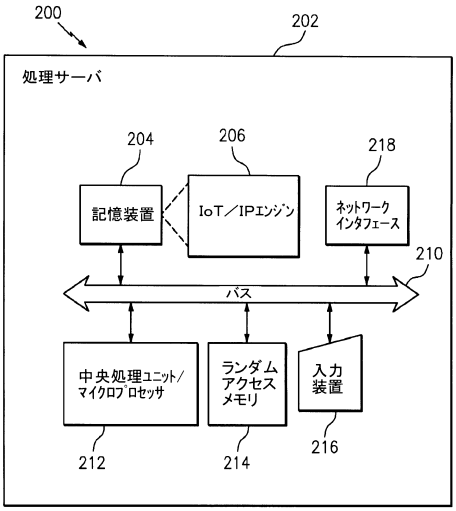
【図６】



【図７】


100
開始
1つまたは複数のログコンシューマとペアリングされたログジェネレータからデータパケットを受信する。
102
受信したデータパケットがIoT/IPシステムのサーバの公開キーにより暗号化されている場合は、これを復号する。
104
受信したデータパケットを処理して、RSIDと(暗号化された)ペイロードを特定する。
106
データパケットのIPアドレスおよび/または受信時間を記録する。
108
データパケットをデータベースに保存する。
110
ログコンシューマからの問い合わせを電子的に受信する。
112
要求されたログエントリをデータベースから電子的に読み出す。
114
ログエントリをログコンシューマ電子的に送信する。
116
終了

【図８】


200
202
処理サーバ
204
206
218
記憶装置
IoT／IPエンジン
ネットワークインタフェース
210
バス
中央処理ユニット/マイクロプロセッサ
ランダムアクセスメモリ
入力装置
212
214
216

フロントページの続き

(56)参考文献 米国特許第０７９９０９６７（ＵＳ，Ｂ２）
特開２００５－１８４３２２（ＪＰ，Ａ）
特開２００９－１６４９０１（ＪＰ，Ａ）
特開２０１５－１７０２８６（ＪＰ，Ａ）
特表２０１１－５０１６２４（ＪＰ，Ａ）
特表２０１６－５００２１０（ＪＰ，Ａ）
米国特許出願公開第２０１３／００９５７５３（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２８，１２／４４－１２／９５５
Ｇ０６Ｆ１３／００