(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2021-69113
(P2021-69113A)
(43)公開日　令和3年4月30日(2021.4.30)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/32	(2006.01)	H04L 9/00	675B	
G06F 21/44	(2013.01)	G06F 21/44		
H04L 9/08	(2006.01)	H04L 9/00	601F	

審査請求 未請求　請求項の数 15　ＯＬ　外国語出願　（全 22 頁）

(21)出願番号　特願2020-174822 (P2020-174822)
(22)出願日　令和2年10月16日 (2020.10.16)
(31)優先権主張番号　19204398.2
(32)優先日　令和1年10月21日 (2019.10.21)
(33)優先権主張国・地域又は機関
欧州特許庁 (EP)

(71)出願人　520405101
エキサーティフィード・アーベー
Ｘｅｒｔｉｆｉｅｄ　ＡＢ
スウェーデン国、１２８　３０　スカールパナック、ホリソントバーゲン　６０
Ｈｏｒｉｓｏｎｔｖａｅｇｅｎ　６０，１２８　３０　Ｓｋａｒｐｎａｅｃｋ，Ｓｗｅｄｅｎ
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100179062
弁理士　井上　正

最終頁に続く

(54)【発明の名称】通信信号を受信及び送信するためのシステム及び方法

(57)【要約】　（修正有）
【課題】データネットワークのセキュリティ、管理可能性、制御可能性、拡張可能性、及び／又は低減可能性を改善する。
【解決手段】通信信号を受信及び送信する通信システム１００であって、データネットワーク１１０、デジタル証明書認証のために構成される少なくとも１つのプロキシデバイス１２０、少なくとも１つのリソース１３０と、を備える。少なくとも１つのプロキシデバイス１２０のうちの各プロキシデバイス１２０は、少なくとも１つのリソース１３０のうちのそれぞれのリソース１３０に結合される。少なくとも１つのリソース１３０は、少なくとも１つのプロキシデバイス１２０を介してデータネットワーク１１０に通信可能に結合される。少なくとも１つのプロキシデバイス１２０は、デジタル証明書認証に基づいて、データネットワーク１１０と少なくとも１つのリソース１３０との間の通信を制御する。
【選択図】図１

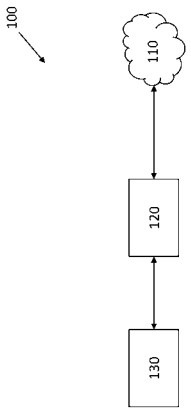

Fig. 1

【特許請求の範囲】
【請求項１】
通信信号を受信及び送信するための通信システムであって、
データネットワークと、
前記データネットワークに結合された少なくとも２つのプロキシデバイスと、ここにおいて、前記少なくとも２つのプロキシデバイスは、デジタル証明書認証のために構成される、
少なくとも２つのリソースと
を備え、前記少なくとも２つのプロキシデバイスのうちの各プロキシデバイスは、前記少なくとも２つのリソースのうちのそれぞれのリソースに結合され、前記少なくとも２つのリソースは、前記少なくとも２つのプロキシデバイスを介して前記データネットワークに通信可能に結合され、前記少なくとも２つのリソースとの通信のための唯一のチャネルは、前記それぞれのプロキシデバイスを通り、前記少なくとも２つのプロキシデバイスは、デジタル証明書認証に基づいて、前記データネットワークと前記少なくとも２つのリソースとの間の通信を制御するように構成される、通信システム。
【請求項２】
前記少なくとも２つのプロキシデバイスは、少なくとも１つのデジタル証明書を記憶するように構成される、請求項１に記載の通信システム。
【請求項３】
前記少なくとも２つのプロキシデバイスは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを生成するように構成される、請求項１又は２に記載の通信システム。
【請求項４】
前記少なくとも２つのプロキシデバイスは、証明書デバイス、パスワード、ＩＰアドレス、ＩＰポート、及びＭＡＣアドレスのうちの少なくとも１つに基づいて、前記データネットワークと前記少なくとも２つのリソースとの間の通信を制御するように更に構成される、請求項１～３のうちのいずれか一項に記載の通信システム。
【請求項５】
前記少なくとも２つのプロキシデバイスは、前記少なくとも２つのリソースに結合された第１の通信ポートと、前記データネットワークに結合された第２の通信ポートとを備える、請求項１～４のうちのいずれか一項に記載の通信システム。
【請求項６】
前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つは、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの識別情報及び位置のうちの少なくとも１つを示すように構成された識別装置を備える、請求項１～５のうちのいずれか一項に記載の通信システム。
【請求項７】
前記識別装置は、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの位置を受信するための受信機を備える、請求項６に記載の通信システム。
【請求項８】
通信装置であって、
請求項１～７のうちのいずれか一項に記載の通信システムと、
前記少なくとも２つのプロキシデバイスに結合された管理システムと、ここにおいて、前記管理システムは、前記少なくとも２つのプロキシデバイスと前記管理システムとの間でデジタル証明書認証データを通信するように構成される、
を備える、通信装置。
【請求項９】
前記少なくとも２つのプロキシデバイスは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを生成するように構成され、

前記管理システムは、前記少なくとも１つの公開鍵及び前記少なくとも１つの私有鍵のうちの少なくとも１つを記憶するように構成される、請求項８に記載の通信装置。
【請求項１０】
前記管理システムは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵を生成するように構成され、前記少なくとも１つの公開鍵及び前記少なくとも１つの私有鍵のうちの少なくとも１つに基づいて、少なくとも１つのデジタル証明書を生成するように更に構成される、請求項８に記載の通信装置。
【請求項１１】
前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つは、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの識別情報及び位置のうちの少なくとも１つを示すように構成された識別装置を備え、
前記管理システムは、前記識別装置に基づいて、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つを実行するように構成される、請求項８に記載の通信装置。
【請求項１２】
前記管理システムは、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの分析と、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの追跡と、前記少なくとも２つのプロキシデバイス及び前記少なくとも２つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの制御とのうちの少なくとも１つを実行するように更に構成される、請求項１１に記載の通信装置。
【請求項１３】
前記管理システム及び前記少なくとも２つのプロキシデバイスのうちの少なくとも１つは、前記データネットワークと前記少なくとも２つのプロキシデバイスとの間のデータ通信を登録するように構成される、請求項８～１２のうちのいずれか一項に記載の通信装置。
【請求項１４】
登録されたデータ通信は、タイムスタンプ、前記少なくとも２つのリソースから前記データネットワークへのデータ、前記データネットワークから前記少なくとも２つのリソースへのデータ、データ通信の送信機、データ通信の受信機、前記データ通信の量、前記データ通信のタイプ、データ通信タイムアウトの数、データ通信試行の数、及び証明書データのうちの少なくとも１つを備える、請求項１３に記載の通信装置。
【請求項１５】
前記管理システム及び前記少なくとも２つのプロキシデバイスのうちの少なくとも１つは、前記登録されたデータ通信に基づいて、前記データネットワークと前記少なくとも２つのプロキシデバイスとの間の前記通信を制御するように更に構成される、請求項１３又は１４に記載の通信装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、通信信号を受信及び送信することに関する。より具体的には、本発明は、通信信号を受信及び送信するためのシステム及び方法に関する。
【背景技術】
【０００２】
接続デバイス及びモノのインターネットへの関心が、製造、医療、及び金融の分野内など、実質的に全ての分野内で着実に増大している。これらの用途の多くのためのネットワークセキュリティは優先されるべきであるが、現在、様々なセキュアでないネットワークに接続されている何千万又は何億ものデバイスが存在する。接続デバイスは、例えば、医

療機器から製造ロボット、交通信号機、プリンタ及びスキャナに及び得る。
【０００３】
ネットワーク及び接続デバイスのための既存のセキュリティソリューションは主に、いくつかの原理に基づく。そのようなネットワーク及び接続デバイスのための１つの原理は、セキュリティをネットワークレベルに設定することを備え得、それによって、ネットワーク内の全てのユーザ及びデバイスが信頼できると想定する。しかしながら、侵入者がネットワークを危険にさらす場合、又はネットワーク内のデバイスがパブリックネットワークに直接接続される場合、ネットワーク上の全てのデバイスが危険にさらされ得る。別の原理は、異なる使用及び／又は技術のクラスタリングであり得、次いで、クラスタのセキュア化に重点を置いている。しかしながら、問題（１つ以上）がそれによって、より多数のより小さい問題に分解され得、それは、セキュリティ閾値を下げる。追加の原理は、特定のハードウェア用にセキュリティを調整することである。しかしながら、そのような調整されたセキュリティソリューションは、他のデバイスもセキュア化されることを許可しないことがある。更に、原理は単純に、セキュアソケットレイヤ（ＳＳＬ）などの比較的低レベルのセキュリティを使用することであり得る。
【０００４】
特許出願第ＵＳ２００３０１９６０８４Ａ１号は、ワイヤレスデバイス上に危険な情報を記憶することなく、セキュアなネットワークとのセキュアな通信に参加するワイヤレスデバイスのシステムを開示している。ワイヤレスデバイスは、いわゆる公開鍵基盤（ＰＫＩ）に参加することを許可され得る。更に、該出願は、アクセスが許可される前に認証（authentication）のためにデジタル証明書（certificate）を提供することをユーザはどのように要求されるかを開示している。しかしながら、ここに開示されるシステムに関連する問題は、それがプロキシサーバとリソースとの間の接続のセキュリティリスクに完全に対処するわけではないことである。例えば、開示されるシステムは、プロキシサーバとリソースとの間の中間者攻撃、即ち、盗聴のリスクがある。ここに開示されるシステムに関連する追加の問題は、プロキシサーバが危険にさらされる場合、全ての接続リソースが危険にさらされ得るということである。
【発明の概要】
【０００５】
それらのセキュリティ及び管理可能性を改善するために、先行技術のネットワークセキュリティソリューションに代替案を提供することは重要である。加えて、特に、レガシーデバイス及び異なる製造業者からのデバイスにとって、パブリック及びプライベートネットワーク中のデバイスの保護を容易することが望まれる。より具体的には、先行技術によるシステムは、十分にセキュアではないことがあり、それらは、異なる技術及び／又は技法の膨大な組み合わせを必要とし得、システムを複雑にし、及び／又は管理を困難にする。加えて、先行技術によって提供されるソリューションをセキュアに拡張又は低減することは難しくあり得る。更に、先行技術によるシステムは、ネットワークへのアクセスを既に有している悪意を持った人物に関して十分にセキュアではないことがある。
【０００６】
故に、本発明の目的は、それらのセキュリティ、管理可能性、制御可能性、拡張可能性、及び／又は低減可能性を改善するために、先行技術のネットワークセキュリティソリューションに代替案を提供することである。
【０００７】
この及び他の目的は、本願独立請求項における特徴を有する通信システムを制御するための通信システム及び方法を提供することによって達成される。好ましい実施形態が、本願従属請求項に規定される。
【０００８】
故に、本発明の第１の態様によると、通信信号を受信及び送信するための通信システムが提供される。通信システムは、データネットワークと少なくとも１つのプロキシデバイスとを備える。少なくとも１つのプロキシデバイスは、データネットワークに結合される

。更に、少なくとも１つのプロキシデバイスは、デジタル証明書認証のために構成される。通信システムは、少なくとも１つのリソースを更に備える。少なくとも１つのプロキシデバイスのうちの各プロキシデバイスは、少なくとも１つのリソースのうちのそれぞれのリソースに結合される。更に、少なくとも１つのリソースは、少なくとも１つのプロキシデバイスを介してデータネットワークに通信可能に結合される。その上、少なくとも１つのプロキシデバイスは、デジタル証明書認証に基づいて、データネットワークと少なくとも１つのリソースとの間の通信を制御するように構成され得る。

【０００９】

本発明の第２の態様によると、通信装置（communication arrangement）が提供される。通信装置は、本発明の第１の態様による通信システムを備える。更に、通信装置は、通信システムの少なくとも１つのプロキシデバイスに結合された管理システムを備える。管理システムは、少なくとも１つのプロキシデバイスと管理システムとの間でデジタル証明書認証データを通信するように構成され得る。

【００１０】

本発明概念の第３の態様によると、通信システムを制御するための方法が提供される。方法は、本発明の第１の態様及び第２の態様のうちの少なくとも１つによる通信システムを備える。方法は、少なくとも１つのプロキシデバイスと、少なくとも１つのリソース及びデータネットワークのうちの少なくとも１つとの間の通信を検出するステップを備える。更に、方法は、デジタル証明書認証を実行するステップを備える。加えて、方法は、デジタル証明書認証に基づいて、検出された通信を制御するステップを備える。

【００１１】

このことから、本発明の第１、第２、及び第３の態様は、１つ以上のリソースがそれぞれのプロキシデバイスを介してデータネットワークに通信可能に結合され、その上、それぞれのプロキシデバイスがデジタル証明書認証に基づいてデータネットワークと少なくとも１つのリソースとの間の通信を制御するように構成され得るという共通概念又は考えに基づく。それによって、各リソースは、それぞれのプロキシデバイスによってセキュア化される。故に、リソースが危険にさらされケースであっても、データネットワークは、依然として保護されるであろう。更に、データネットワークが危険にさらされるケースであっても、各リソースは、依然としてそれぞれのプロキシデバイスによって保護される。本発明はそれによって、より高いレベルの冗長性を有し、それは、セキュリティのレベルを増大させる。それによって、ある人物が保護されたプライベートネットワーク又はプロキシサーバを危険にさらすことになっても、通信可能に結合されたリソースは、依然として各それぞれのプロキシデバイスによって保護されるであろう。

【００１２】

通信システムは、システム内で、並びに通信システムと他のデバイス及び／又はネットワークとの間で、通信信号を受信及び送信するように構成され得る。通信システムは、通信信号をセキュアに受信及び送信するように構成され得る。通信システムは、データネットワーク、データネットワークに結合された少なくとも１つのプロキシデバイス、及び少なくとも１つのリソースを備える。「データネットワーク」という用語は、ここでは、単一のセキュアなデータネットワーク、単一のセキュアでないデータネットワーク、クラウドデータネットワーク、及び複数の補助データネットワークのうちの少なくとも１つを意味する。「プロキシデバイス」という用語は、ここでは、データネットワークと少なくとも１つのリソースとの間の通信を制御するように構成された中間デバイスを意味する。より具体的には、「プロキシデバイス」は、通信ゲートキーピングのために構成されたデバイスを構成し得る。

【００１３】

少なくとも１つのプロキシデバイスは、デジタル証明書認証のために構成される。「デジタル証明書認証」という用語は、ここでは、例えば、電子文書、デジタル証明書、シグネチャ、公開鍵、及び／又は私有鍵のうちの少なくとも１つに基づく、セキュアな通信の認証又は確証（validation）を意味する。「リソース」という用語は、ここでは、データ

ネットワークに通信可能に結合され得る実質的に任意のデバイス、例えば、電子デバイスを意味する。少なくとも１つのプロキシデバイスは、デジタル証明書認証に基づいて、データネットワークと少なくとも１つのリソースとの間の通信を制御するように構成される。「通信を制御するように構成される」という用語は、ここでは、プロキシデバイスが通信を許可されるか又は許可されないように構成されることを意味する。

【００１４】

本発明の実施形態によると、少なくとも１つのプロキシデバイスは、少なくとも１つのデジタル証明書を記憶するように構成され得る。「デジタル証明書」という用語は、ここでは、電子文書、アイデンティティ証明書、シグネチャ、公開鍵（public key）、及び／又は私有鍵（private key）のうちの少なくとも１つを意味する。少なくとも１つのプロキシデバイスは、１つ以上の記憶されるデジタル証明書（１つ以上）に少なくとも基づいて、データネットワークと少なくとも１つのリソースとの間の通信を制御するように構成され得る。記憶される証明書（１つ以上）は、通信システムによって生成され得ることに留意されたい。本実施形態は、通信システムのセキュリティが更に一層増大し得るという点において有利である。更に、通信システムの管理可能性が増大し得る。少なくとも１つのプロキシデバイスは、第１のモードと呼ばれ得る少なくとも１つのデジタル証明書を記憶するように構成され得る。第１のモードで動作するように構成されたプロキシデバイスは、特に、それが少なくとも１つのデジタル証明書を生成するように構成されたプロキシデバイスよりも少ない量の計算電力を必要とし得るという点において、比較的エネルギー効率が良くあり得ることが認識されるであろう。従って、第１のモードで動作するように構成されたプロキシデバイスは、より少ない電力を消費し得、更に比較的小さくあり得る。その上、第１のモードで動作するように構成されたプロキシデバイスは、そのそれぞれのリソースに近接してより好都合に配置され得る。

【００１５】

本発明の実施形態によると、少なくとも１つのプロキシデバイスは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを生成するように構成され得る。少なくとも１つのプロキシデバイスは、アクティブモードと呼ばれ得る第２のモードで動作するように構成され得る。第２のモードで動作するように構成されたプロキシデバイスは、１つ以上の公開鍵（１つ以上）及び／又は１つ以上の私有鍵（１つ以上）を生成するように構成され得る。少なくとも１つのプロキシデバイスは、公開鍵（１つ以上）及び／又は私有鍵（１つ以上）に基づいてデジタル証明書を受信するように構成され得る。故に、本実施形態は、通信システムのセキュリティが更に一層増大し得るという点において有利である。

【００１６】

本発明の実施形態によると、少なくとも１つのプロキシデバイスは、証明書ハードウェア、パスワード、ＩＰアドレス、ＩＰポート、及びＭＡＣアドレスのうちの少なくとも１つに基づいて、データネットワークと少なくとも１つのリソースとの間の通信を制御するように更に構成され得る。故に、少なくとも１つのプロキシデバイスは、デジタル証明書認証と、証明書ハードウェア、パスワード、ＩＰアドレス、ＩＰポート、及びＭＡＣアドレスのうちの１つ以上とに基づいて、データネットワークとリソース（１つ以上）との間の通信を制御するように更に構成され得る。システムのセキュリティのレベルは、システムの通信の制御が基づくこれらの述べられた特徴又は機能の全ての追加によって増大し得ることが認識されるであろう。

【００１７】

本発明の実施形態によると、少なくとも１つのプロキシデバイスは、少なくとも１つのリソースに結合された第１の通信ポートと、データネットワークに結合された第２の通信ポートとを備え得る。故に、１つ以上のリソース（１つ以上）は、それぞれの１つ以上のプロキシデバイス（１つ以上）の第１及び第２の通信ポートを介してデータネットワークに物理的に結合され得る。リソース（１つ以上）との通信は従って、プロキシデバイスを通って、又は第１及び第２の通信ポートを介したリソースへの直接の物理的結合によって

のみ可能である。リソース（１つ以上）への直接の物理的結合又は接続は、１つ以上のリソース（１つ以上）への物理的アクセスが存在することを必要とし、それは制限され得ることが認識されるであろう。それによって、通信システムのセキュリティは、本実施形態によって更に一層増大し得る。

【００１８】

本発明の実施形態によると、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つは、識別装置（identifier）を備え得る。識別装置は、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの識別情報及び位置のうちの少なくとも１つを示すように構成され得る。「識別装置」という用語は、ここでは、プロキシデバイス（１つ以上）及び／又はリソース（１つ以上）の識別情報又は位置を示すように構成された、実質的に任意のデバイス、ユニット、又は同様のものを意味する。システムのセキュリティは、どのユーザ（１人以上）及び／又はデバイス（１つ以上）がシステム中にいる／あるのか、及びこれらのユーザ（１人以上）及び／又はデバイス（１つ以上）がシステム中のどこにいる／あるのかを知っていることに依存し得ることに留意されたい。故に、少なくとも１つのリソース及び／又は少なくとも１つのプロキシデバイスが識別及び／又は位置推定される（localized）通信システムは、通信システムのセキュリティを更に増大させ得る。

【００１９】

本発明の実施形態によると、識別装置は、受信機を備え得る。受信機は、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの位置を受信するように構成され得る。それによって、プロキシデバイス（１つ以上）及び／又はリソース（１つ以上）は、地理的に位置推定され得、それは、システムの制御可能性及びセキュリティを更に増大させ得る。

【００２０】

本発明の実施形態によると、管理システムは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを記憶するように構成され得る。管理システムが公開鍵（１つ以上）及び／又は私有鍵（１つ以上）を記憶するように構成される場合、少なくとも１つのプロキシデバイスは、これらの公開鍵（１つ以上）及び／又は私有鍵（１つ以上）を記憶するように構成される必要はないことがあることが認識されるであろう。本実施形態は、プロキシデバイスがその構成においてより複雑でないことがあるという点において有利である。例えば、本実施形態によるプロキシデバイスは、公開鍵（１つ以上）及び／又は私有鍵（１つ以上）を記憶するように構成されたプロキシデバイスよりも少ない（複雑な）ハードウェア／回路を備え得る。故に、プロキシデバイスのエネルギー消費が低減され得る。更に、プロキシデバイスのサイズが低減され得る。加えて、そのようなプロキシデバイスを生産するのに必要とされる材料の量（要素）が低減され得、それによって、システムのコスト効率を改善する。

【００２１】

本発明の別の実施形態によると、管理システムは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵を生成するように構成され得る。管理は、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つに基づいて少なくとも１つのデジタル証明書を生成するように更に構成され得る。故に、管理システムは、公開鍵（１つ以上）及び／又は私有鍵（１つ以上）を生成し、プロキシデバイス（１つ以上）にこの鍵又はこれらの鍵を提供するように構成され得る。それ故に、プロキシデバイスは、この鍵又はこれらの鍵自体を生成するように構成される必要がないことがある。

【００２２】

本実施形態は、システムの効率が更に一層増大し得るという点において有利である。

【００２３】

本発明の実施形態によると、管理システムは、識別装置に基づいて、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つを実行するように構成され得る。言い換えれば、本通信装置

は、通信システムを備え得、ここにおいて、リソース（１つ以上）及び／又はプロキシデバイス（１つ以上）は、識別装置に基づいて識別及び／又は位置推定される。本実施形態は、リソース（１つ以上）及び／又はプロキシデバイス（１つ以上）の識別及び／又は位置推定（localization）が通信装置のセキュリティを更に一層増大させ得るという点において有利である。

【００２４】

本発明の実施形態によると、管理システムは、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つの分析と、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つの追跡と、少なくとも１つのプロキシデバイス及び少なくとも１つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つの制御とのうちの少なくとも１つを実行するように更に構成され得る。本実施形態のプロキシデバイス（１つ以上）及び／又はリソース（１つ以上）の識別及び／又は位置推定の分析、追跡、及び／又は制御は、通信システムの透明性を増大させ得ることが認識されるであろう。故に、この実施形態によって、通信装置のセキュリティ及び／又は制御可能性が更に一層増大し得る。

【００２５】

本発明の実施形態によると、管理システム及び少なくとも１つのプロキシデバイスのうちの少なくとも１つは、データネットワークと少なくとも１つのプロキシデバイスとの間のデータ通信を登録するように構成され得る。故に、管理システム及び／又はプロキシデバイス（１つ以上）は、データネットワークとプロキシデバイス（１つ以上）との間の、即ち、それぞれ、プロキシデバイスからデータネットワークへの、及びデータネットワークからプロキシデバイスへの、データ通信を登録するように構成され得る。「登録するように構成される」という用語は、管理システム及び／又はプロキシデバイス（１つ以上）がデータネットワークとプロキシデバイス（１つ以上）との間のデータ通信を記録、目録化（catalogue）、及び／又は書き留め（note）得ることを意味する。通信装置による登録されたデータ通信は、通信の制御可能性を改善するために使用され得、それによって、通信装置のセキュリティを増大させる。

【００２６】

登録されたデータ通信は、タイムスタンプ、少なくとも１つのリソースからネットワークへのデータ、データネットワークから少なくとも１つのリソースへのデータ、データ通信の送信機（sender）、データ通信の受信機、データ通信の量、データ通信のタイプ、データ通信タイムアウトの数、データ通信試行の数、及び証明書データのうちの少なくとも１つを備え得る。言い換えれば、登録されたデータは、例証されたように、述べられたデータ形式のうちの任意のもの、又は組み合わせを備え得る。故に、本実施形態によって、通信の制御可能性、及びそれによって、通信装置のセキュリティが更に一層増大し得る。

【００２７】

本発明の実施形態によると、管理システム及び少なくとも１つのプロキシデバイスのうちの少なくとも１つは、登録されたデータ通信に基づいて、データネットワークと少なくとも１つのプロキシデバイスとの間の通信を制御するように更に構成され得る。故に、本実施形態によると、管理システム及びプロキシデバイス（１つ以上）は、前述された実施形態のうちの１つ以上に従って、登録されたデータ通信に基づいて通信を制御するように構成され得る。本実施形態は、通信装置中のセキュリティのレベルが増大するという点において有利である。

【００２８】

本発明の実施形態によると、管理システム及び少なくとも１つのプロキシデバイスのうちの少なくとも１つは、データネットワークと少なくとも１つのプロキシデバイスとの間のデジタル証明書データを登録するように構成され得る。登録されたデジタル証明書データは、タイムスタンプ、少なくとも１つのプロキシデバイスからデータネットワークに送信されるデジタル証明書、データネットワークから少なくとも１つのプロキシデバイスに

送信されるデジタル証明書、少なくとも１つのプロキシデバイスによって受信されるデジタル証明書、データネットワークによって受信されるデジタル証明書、デジタル証明書要求の数のうちの少なくとも１つを備え得る。故に、本実施形態によって、通信システムのセキュリティが改善され得る。

【００２９】

ここで、本発明のこの及び他の態様が、本発明の実施形態（１つ以上）を示す添付された図面を参照して、より詳細に説明されることになる。

【図面の簡単な説明】

【００３０】

【図１】本発明の例証的な実施形態による通信システムを概略的に示す。

【図２】本発明の例証的な実施形態による通信システムを概略的に示す。

【図３】本発明の例証的な実施形態による通信システムを概略的に示す。

【図４】本発明の例証的な実施形態による通信システムを概略的に示す。

【図５】本発明の例証的な実施形態による通信装置を概略的に示す。

【図６】本発明の例証的な実施形態による通信装置を概略的に示す。

【詳細な説明】

【００３１】

図１は、本発明の例証的な実施形態による、通信信号を受信及び送信するための通信システム１００を概略的に示す。示された通信システム１００は、データネットワーク１１０を備える。更に、通信システム１００は、データネットワーク１１０に結合されたプロキシデバイス１２０を備える。通信システム１００は、リソース１３０を備えるように示される。プロキシデバイス１２０は、それぞれのリソース１３０に結合され、即ち、通信システム１００の各プロキシデバイス１２０は、それぞれのリソース１３０に結合される。リソース１３０は、プロキシデバイス１２０を介してデータネットワーク１１０に通信可能に結合される。プロキシデバイス１２０は、デジタル証明書認証のために構成される。示されたプロキシデバイス１２０は、デジタル証明書認証に基づいて、データネットワーク１１０とリソース１３０との間の通信を制御するように更に構成される。

【００３２】

例証されたような通信システム１００は、図１の例示によって限定されないことに留意されたい。例えば、それぞれのいくつかのプロキシデバイス１２０に通信可能に結合され得る実質的に任意の数のリソース１３０であり得る。プロキシデバイス１２０は、ワイヤを介して又はワイヤレスにデータネットワーク１１０に通信可能に結合され得る。加えて、プロキシデバイス１２０は、スイッチ及びルータ（図示せず）を介してデータネットワーク１１０に通信可能に結合され得る。更に、「データネットワーク」という用語は、単一のセキュアなデータネットワーク、単一のセキュアでないデータネットワーク、クラウドデータネットワーク、及び複数の補助データネットワークのうちの少なくとも１つとして解釈されるべきである。

【００３３】

例によると、図１のプロキシデバイス１２０は、少なくとも１つのデジタル証明書４１０（図示せず）を記憶するように構成され得、ここにおいて、少なくとも１つのデジタル証明書は、デジタル証明書認証のために使用され得る。更に、プロキシデバイス１２０は、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを生成するように構成され得、ここにおいて、公開鍵（１つ以上）及び／又は私有鍵（１つ以上）は、デジタル証明書認証のために使用され得る。更に、プロキシデバイス１２０は、証明書デバイス、パスワード、ＩＰアドレス、ＩＰポート、及びＭＡＣアドレスのうちの１つ以上に基づいて、データネットワーク１１０とリソース（１つ以上）１３０との間の通信を制御するように更に構成され得る。

【００３４】

図１には明示的に示されないが、データネットワーク１１０は、複数の補助データネットワークを備え得、ここにおいて、この複数の補助データネットワークは、通信可能に相

互接続され得ることが認識されるであろう。例えば、リソース１３０は、プロキシデバイス１２０を介して第１の補助データネットワークに通信可能に結合され得、プロキシデバイス１２０は、例えば、第２の補助データネットワークから受信されたデジタル証明書認証に基づいて、第１の補助データネットワークとリソース１３０との間の通信を制御するように構成され得る。

【００３５】

図２は、本発明の例証的な実施形態による、通信信号を受信及び送信するための通信システム１００を概略的に示す。図２は、図１に示され、関連するテキストに説明されたような特徴、要素、及び／又は機能を備えることに留意されたい。故に、理解を深めるために、その図及びテキストも参照される。

【００３６】

図２では、示された通信システム１００のデータネットワーク１１０は、デジタル証明書サーバ４００に通信可能に結合される。明確さの理由から別個に描かれているが、データネットワーク１１０はデジタル証明書サーバ４００を備え得ることが理解されるべきである。デジタル証明書サーバ４００は、公開鍵及び／又は私有鍵に基づいてデジタル証明書を生成するように構成され得る。デジタル証明書サーバ４００は、公開鍵基盤（ＰＫＩ）デバイスを備え得る。更に、ＰＫＩデバイスは、ネットワーク認証サーバ（ＮＡＳ）又はネットワークサーバ（ＮＳ）を備え得る。通信システム１００は、デジタル証明書サーバ４００との通信に基づいて、デジタル証明書認証のために構成され得る。通信システム１００のプロキシデバイス１２０は、デジタル証明書サーバ４００に通信可能に結合され得る。プロキシデバイス１２０とデジタル証明書サーバ４００との間の通信可能な結合は、データネットワーク１１０を介して提供され得る。プロキシデバイス１２０は、デジタル証明書サーバ４００との通信に基づいて、デジタル証明書認証のために構成され得る。プロキシデバイス１２０は、ネットワークアドレス変換（ＮＡＴ）のために構成され得る。

【００３７】

図２に例示されているのは、プロキシデバイス１２０とデータネットワーク１１０との間のデジタル証明書４１０の送信である。プロキシデバイス１２０は、それぞれのリソース１３０がプロキシデバイス１２０を介して通信することを試みる場合、デジタル証明書４１０を送信するように構成され得る。デジタル証明書４１０は、デジタル証明書サーバ４００にデータネットワーク１１０を介して送信され得る。デジタル証明書サーバ４００は、デジタル証明書４１０を認証するように構成され得る。「認証する（authenticate）」という用語は、確証する（validate）、承認する（approve）、証明する（certify）、確認する（confirm）、及び／又は実証する（verify））、を少なくとも備えることが理解されるべきである。プロキシデバイス１２０は、デジタル証明書サーバ４００によるデジタル証明書認証に基づいて、データネットワーク１１０とリソース１３０との間の通信を制御するように構成され得る。プロキシデバイス１２０は、デジタル証明書認証に基づいて、リソース１３０とデータネットワーク１１０との間の通信を許可するか又は拒否するかのいずれかを行うように更に構成され得る。プロキシデバイス１２０は、ＩＰポート、ＩＰフィルタ、及び／又はポートフィルタのうちの１つ以上に基づいて通信を制御するように更に構成され得る。

【００３８】

例によると、通信システム１００は、所定のデータネットワークインシデント（incident）に基づいてリソース（１つ以上）１３０の取り消し、隔離、及び／又は切断を行うように構成され得る。「データネットワークインシデント」という用語は、データネットワーク１１０、プロキシデバイス（１つ以上）１２０、リソース（１つ以上）１３０、及び／又はデジタル証明書サーバ４００の間の送信における切断及び／又は変化など、通信システム１００中の実質的に任意の種類のインシデント、イベント、変化、又は同様のものを意味する。

【００３９】

図２に示されたプロキシデバイス１２０は、リソース１３０に通信可能に結合された第１の通信ポート２１０を更に備える。更に、示されたプロキシデバイス１２０は、データネットワーク１１０に通信可能に結合された第２の通信ポート２２０を備える。プロキシデバイス１２０は、第１の通信ポート２１０及び第２の通信ポート２２０を介して通信を制御するように構成され得る。ここで、リソース１３０は、第１の通信ポート２１０を介してのみプロキシデバイス１２０に通信可能に結合され得る。故に、リソース１３０との通信のための唯一のチャネルは、それぞれのプロキシデバイス１２０を通り得る。第１及び／又は第２の通信ポート２１０、２２０は、任意の特定の種類のポート及び／又はインターフェースに限定されないことが認識されるであろう。第１及び／又は第２の通信ポート２１０、２２０は、ＲＪ４５、ワイヤレス、ファイバ、ＵＳＢ、及びＲＳ２３２のうちの少なくとも１つを備え得る。プロキシデバイス１２０は、１つの（即ち、単一の）通信チャネルを備え得る。通信チャネルは、リソース１３０に結合された第１の通信ポート２１０と、データネットワーク１１０に結合された第２の通信ポート２２０とを備え得る。それによって、通信システム１００中には一方向通信のみが存在し得、即ち、プロキシデバイス１２０を通る。

【００４０】

図２に例証されたような通信システム１００によると、プロキシデバイス１２０は、識別装置３００を備えるように示される。識別装置３００は、プロキシデバイス１２０の識別情報及び／又は位置を示すように構成され得る。リソース１３０は、識別装置３００を備え得ることに留意されたい。更に、示された識別装置３００は、受信機３１０を備える。受信機３１０は、プロキシデバイス１２０の位置を受信するように構成され得る。更に、受信機３１０は、プロキシデバイス１２０に位置を送信するように構成され得る。次に、プロキシデバイス１２０は、データネットワーク１１０に位置を送信するように構成され得る。受信機３１０は、位置を記憶するように構成され得る。更に、受信機３１０は、ＧＰＳ位置を受信するように構成され得る。

【００４１】

識別装置３００は、可読コード（図示せず）を備え得る。可読コードは、例えば、バーコード、ＱＲコード（登録商標）、又は同様のものとして構成され得る。識別装置３００は、可読及び／又は走査可能であるように構成され得る。更に、識別装置３００は、ハンドヘルドデバイスによって読み取られる及び／又は走査されるように構成され得る。識別情報のインジケーションは、識別番号、シリアル番号、及びデバイス名のうちの１つ以上を備え得る。識別装置３００は、プロキシデバイス１２０と（直接物理的に）接触していることがある。

【００４２】

加えて、例証されたような識別情報のインジケーションは、デジタルＩＤと呼ばれ得る、識別情報のデジタルインジケーションを備え得ることが認識されるであろう。デジタルＩＤは、ＩＰアドレス、ＩＰポート、データネットワーク内の位置、接続デバイスの識別データ、及びＭＡＣアドレスのうちの少なくとも１つを備え得る。更に、プロキシデバイス１２０及びリソース１３０、並びにデータネットワーク１１０内の及び／又はデータネットワーク１１０へのそれらの結合及び／又は接続が、詳細に示され得る。故に、通信システム１００の１つ以上のデバイス、接続、等の変化は、追跡及び監視されることができる。

【００４３】

プロキシデバイス１２０及び／又はリソース１３０の位置のインジケーションは、プロキシデバイス１２０及び／又はリソース１３０の地理的位置を示すことを備え得る。代替として、少なくとも１つのプロキシデバイス１２０及び／又はリソース１３０の位置のインジケーションは、プロキシデバイス１２０及び／又はリソース１３０のネットワーク位置を示すことを備え得る。通信システム１００は、プロキシデバイス１２０及び／又はリソース１３０の（地理的及び／又はネットワーク）位置のインジケーションを受信するように構成され得る。

【００４４】
更に、通信システム１００は、ブループリントを備え得る。「ブループリント」という用語は、例えば、図面、設計、及び／又はコンピュータ支援設計（ＣＡＤ）ファイルなどのデータ及び／又はファイルを備えることが理解されるべきである。ブループリントは、リソース１３０及び／又はプロキシデバイス１２０が位置する地理的場所（１つ以上）に関する情報を備え得る。更に、ブループリントは、１つのリソース１３０及び／又はプロキシデバイス１２０が該地理的場所（１つ以上）中に位置するという情報及び／又はインジケーション（１つ以上）を備え得る。
【００４５】
図３は、本発明の例証的な実施形態による、通信信号を受信及び送信するための通信システム１００を示す。図３は、図１及び２に関連して示され、説明されたような特徴、要素、及び／又は機能を備えることに留意されたい。故に、理解を深めるために、それらの図及び関連するテキストも参照される。
【００４６】
図３の例示された通信システム１００は、理解の理由のために例証的である。例えば、実質的に任意の数のリソース１３０があり得る。それ故に、通信システム１００は、データネットワーク１１０に結合された任意の数のプロキシデバイス１２０を備え得、ここにおいて、各プロキシデバイス１２０は、それぞれのリソース１３０に結合される。通信システム１００のデータネットワーク１１０は、２つのユーザデバイス１４０ａ、１４０ｂに通信可能に結合される。「ユーザデバイス」という用語は、ここでは、データネットワーク１１０を介してリソース１３０に接続するように構成された実質的に任意の（電子）デバイス、例えば、コンピュータを意味する。通信システム１００のデータネットワーク１１０に結合された実質的に任意の数のユーザデバイス１４０ａ、１４０ｂがあり得、２つのユーザデバイス１４０ａ、１４０ｂが例として示されることが認識されるであろう。図３の例によると、データネットワーク１１０に結合されたユーザデバイス１４０ａ、１４０ｂと、それぞれのプロキシデバイス１２０を介してデータネットワーク１１０に結合されたリソース１３０との間の通信は、デジタル証明書認証に基づいてプロキシデバイス１２０によって制御され得る。ユーザデバイス（１つ以上）１４０ａ、１４０ｂは、プロキシデバイス１２０を介してのみリソース１３０と通信し得、ここにおいて、プロキシデバイス１２０は、デジタル証明書認証に基づいて、ユーザデバイス（１つ以上）１４０ａ、１４０ｂとリソース１３０との間の通信を制御するように構成される。それによって、認証されたユーザデバイス１４０ａ、１４０ｂのみが、リソース１３０と通信し得る。故に、ユーザデバイス１４０ａ、１４０ｂを使用する悪意を持った人物が、ユーザデバイス１４０ａ、１４０ｂによってデータネットワーク１１０に接続され得るにもかかわらず、悪意を持った人物は、リソース１３０に接続することができないことがある。
【００４７】
図４は、本発明の例証的な実施形態による、通信信号を受信及び送信するための通信システム１００を示す。図４は、図１、２、及び／又は３に関連して示され、説明されたような特徴、要素、及び／又は機能を備えることに留意されたい。故に、理解を深めるために、それらの図及び関連するテキストのうちの１つ以上も参照される。
【００４８】
図４の通信システム１００は、２つのデジタル証明書４１０ａ、４１０ｂを示す。デジタル証明書４１０ａ、４１０ｂは、ユーザデバイス１４０ａ、１４０ｂとデータネットワーク１１０との間で送信され得る。デジタル証明書４１０ａ、４１０ｂは、データネットワーク１１０を介してユーザデバイス１４０ａ、１４０ｂからプロキシデバイス１２０に送信され得る。リソース１３０がそれを介してデータネットワーク１１０に通信可能に結合されるプロキシデバイス１２０は、デジタル証明書認証に基づいて、リソース１３０とユーザデバイス１４０ａ、１４０ｂとの間の通信を制御するように構成され得、ここにおいて、デジタル証明書認証は、デジタル証明書４１０ａ、４１０ｂのうちの１つ以上に基づき得る。更に、デジタル証明書（１つ以上）４１０ａ、４１０ｂは、パスワード、ＩＰ

アドレス、ＩＰポート、及び／又はＭＡＣアドレスを更に備え得る。
【００４９】
更に、例によると、ユーザデバイス１４０ｂは、証明書デバイス４２０に結合されるように示される。更に、証明書デバイス４２０は、リソース１３０に通信可能に結合され得る。証明書デバイス４２０は、ユーザデバイス１４０ｂに証明書データを提供するように構成され得、ここにおいて、証明書データは、デジタル証明書４１０、パスワード、公開鍵、私有鍵、及びトークンのうちの少なくとも１つを備え得る。加えて、プロキシデバイス１２０は、デジタル証明書認証に基づいてリソース１３０とユーザデバイス１４０ｂとの間の通信を制御するように構成され得、ここにおいて、デジタル証明書認証は、証明書データに少なくとも基づき得る。証明書デバイス４２０は、スマートカードを受信するように構成され得、ここにおいて、スマートカードは、証明書デバイスに証明書データを提供するように構成され得る。「スマートカード」という用語は、デジタル証明書認証のために構成された物理的電子デバイスを意味する。
【００５０】
図４に示されたプロキシデバイス１２０は、デジタル証明書サーバ４００に通信可能に結合される。デジタル証明書サーバ４００は、公開鍵基盤（ＰＫＩ）デバイスを備え得る。更に、ＰＫＩデバイスは、証明書認証サーバ（ＣＡＳ）又は証明書サーバ（ＣＳ）を備え得る。本発明概念は、図４に示された実施形態に限定されないことに留意されたい。例えば、プロキシデバイス（１つ以上）１２０は、データネットワーク１１０を介してデジタル証明書サーバ４００に通信可能に結合され得る。プロキシデバイス（１つ以上）１２０は、デジタル証明書サーバ４００にデジタル証明書４１０を送信するように構成され得る。デジタル証明書サーバ４００は、デジタル証明書４１０を認証し得る。代替として、プロキシデバイス１２０は、デジタル証明書のリストを備え得る。プロキシデバイス１２０は、証明書リストに基づいてデジタル証明書４１０を認証するように構成され得る。ユーザデバイス（１つ以上）１４０ａ、１４０ｂは、デジタル証明書（１つ以上）４１０ａ、４１０ｂに基づいて、プロキシデバイス１２０を介してのみリソース１３０と通信し得ることが認識されるであろう。故に、ユーザデバイス（１つ以上）１４０ａ、１４０ｂを使用する悪意を持った人物は、プロキシデバイス１２０にデジタル証明書（１つ以上）４１０ａ、４１０ｂに提供することなくリソース１３０に接続することができない。
【００５１】
図５は、例証的な例による通信装置５００を示す。示された通信装置５００は、本発明の例証的な実施形態による通信システム１００を備える。図５は、図１～４に関連して示され、説明されたような特徴、要素、及び／又は機能を備えることに留意されたい。故に、理解を深めるために、それらの図及び／又は関連するテキストのうちの１つ以上も参照される。
【００５２】
図５に示された通信装置５００は、管理システム５１０を備える。管理システム５１０は、プロキシデバイス１２０と管理システム５１０との間でデジタル証明書認証データを通信するように構成され得る。更に、図５は、管理装置５１０の管理システム５１０に通信可能に結合されたユーザデバイス１４０を示す。リソース１３０は、プロキシデバイス１２０及び管理システム５１０を介してユーザデバイス１４０に通信可能に結合される。
【００５３】
管理システム５１０は、公開鍵及び／又は私有鍵を記憶するように構成され得る。管理システム５１０は、プロキシデバイス１２０にデジタル証明書を通信するように構成され得、ここにおいて、プロキシデバイス１２０は、デジタル証明書を記憶するように構成され得る。
【００５４】
管理システム５１０及び／又はプロキシデバイス（１つ以上）１２０は、データネットワーク１１０とプロキシデバイス（１つ以上）１２０との間のデータ通信を登録するように構成され得る。登録されたデータ通信は、タイムスタンプ、リソース（１つ以上）１３

０からデータネットワーク１１０へのデータ、データネットワーク１１０からリソース（１つ以上）１３０へのデータ、データ通信の送信機、データ通信の受信機、データ通信の量、データ通信のタイプ、データ通信タイムアウトの数、データ通信試行の数、及び証明書データのうちの１つ以上を備え得る。管理システム５１０及び／又はプロキシデバイス（１つ以上）１２０は、データネットワーク１１０とプロキシデバイス（１つ以上）１２０との間の通信を制御するように更に構成され得る。データネットワーク１１０とプロキシデバイス（１つ以上）１２０との間の通信を制御することは、登録されたデータ通信に基づき得る。登録されたデータ通信は、データネットワークインシデントを備え得る。管理システム５１０及び／又はプロキシデバイス１２０は、所定の登録されたデータ通信に基づいて、データネットワーク１１０とプロキシデバイスとの間の通信を制御するように更に構成され得る。管理システム５１０及び／又はプロキシデバイス１２０は、所定の登録されたデータ通信に基づいて、データネットワーク１１０とプロキシデバイスとの間の通信の所定の制御を実行するように更に構成され得る。管理システム５１０による通信の制御は、プロキシデバイス１２０、リソース１３０、ユーザデバイス１４０、及び／又はデータネットワーク１１０を接続すること、プロキシデバイス１２０、リソース１３０、ユーザデバイス１４０、及び／又はデータネットワーク１１０を切断すること、プロキシデバイス１２０、リソース１３０、ユーザデバイス１４０、及び／又はデータネットワーク１１０を再ルーティングすること、デジタル証明書４１０を取り消すこと、証明書リストを変えること、ポートを閉じること、及び／又はプロキシデバイス１２０、リソース１３０、ユーザデバイス１４０、及び／又はデータネットワーク１１０と、プロキシデバイス１２０、リソース１３０、ユーザデバイス１４０、及び／又はデータネットワーク１１０との間の帯域幅を変更することを備え得る。

【００５５】

ユーザデバイス１４０は、プロキシデバイス１２０及び／又は管理システム５１０を介してのみリソース１３０と通信し得る。プロキシデバイス１２０及び／又は管理システム５１０は、デジタル証明書認証及び／又は登録されたデータ通信に基づいて、ユーザデバイス１４０とリソース１３０との間の通信を制御するように構成され得る。

【００５６】

図６は、本発明の例証的な実施形態による通信装置５００を示す。図６は、図１～５に関連して示され、説明されたような特徴、要素、及び／又は機能を備えることに留意されたい。故に、理解を深めるために、それらの図及び／又は関連するテキストのうちの１つ以上も参照される。

【００５７】

加えて、図６に示された通信装置５００は、デジタル証明書サーバ４００を備える。示されたデジタル証明書サーバ４００は、管理システム５１０及びプロキシデバイス１２０に通信可能に結合される。更に、デジタル証明書サーバ４００は、データネットワーク１１０を介して管理システム５１０及び／又はプロキシデバイス（１つ以上）１２０に通信可能に結合され得る。

【００５８】

通信装置５００は、任意の数のリソース１３０を備え得、ここにおいて、各リソース１３０は、それぞれのプロキシデバイス１２０を介してデータネットワーク１１０に結合される。各プロキシデバイス１２０は、デジタル証明書認証に基づいて、データネットワーク１１０とそのそれぞれのリソース１３０との間の通信を制御するように構成される。

【００５９】

故に、各プロキシデバイス１２０は、デジタル証明書認証に基づいて、データネットワーク１１０からそのそれぞれのリソース１３０への通信を制御するように構成され得る。ユーザデバイス１４０は、通信システム１００のデータネットワーク１１０に結合され得る。それによって、各プロキシデバイス１２０は、デジタル証明書認証に基づいて、ユーザデバイス１４０とプロキシデバイス１２０のそれぞれのリソース１３０との間の通信を制御するように構成され得る。デジタル証明書認証は、プロキシデバイス１２０が管理シ

ステム５１０からデジタル証明書４１０を受信することを備え得る。プロキシデバイス１２０は、受信されたデジタル証明書４１０を証明書リストと比較するように構成され得る。プロキシデバイス１２０及び／又は管理システム５１０は、デジタル証明書４１０と証明書リストとの間の比較に基づいてデジタル証明書４１０を認証するように構成され得る。

【００６０】

管理システム５１０は、デジタル証明書４１０を生成するように構成され得る。加えて、管理システム５１０は、１つ以上の公開鍵（１つ以上）及び／又は１つ以上の私有鍵（１つ以上）を生成するように構成され得る。更に、管理システム５１０は、公開鍵（１つ以上）及び／又は私有鍵（１つ以上）に基づいてデジタル証明書４１０を生成するように構成され得、ここにおいて、この鍵又はこれらの鍵は、管理システム５１０によって生成され得る。

【００６１】

加えて、管理システム５１０は、管理システム５１０からデジタル証明書サーバ４００への１つ以上の公開鍵（１つ以上）及び／又は１つ以上の私有鍵（１つ以上）の送信に基づいて、デジタル証明書サーバ４００からデジタル証明書４１０を受信するように構成され得る。デジタル証明書４１０は、プロキシデバイス１２０のエンロールメント中に生成され得る。「エンロールメント」という用語は、ブートストラップ及び／又はインストールを意味する。証明書リストは、プロキシデバイス１２０のエンロールメント中に生成され得る。プロキシデバイス１２０のエンロールメントは、プロキシデバイス１２０を介してデータネットワーク１１０にそれぞれのリソース１３０を結合することを備え得る。プロキシデバイス１２０のエンロールメントは、デジタル証明書４１０及び／又は証明書リストを生成すること、及び／又はプロキシデバイス１２０中にデジタル証明書４１０及び／又は証明書リストを記憶することを更に備え得る。証明書リストを生成することは、管理システム５１０から証明書リストを受信することを備え得る。リストは、備えられたリソース（１つ以上）１３０及び／又は通信システム１００に結合されたユーザデバイス（１つ以上）１４０に関連するデジタル証明書（１つ以上）４１０を備え得る。管理システム５１０は、デジタル証明書４１０の取り消しのために構成され得る。デジタル証明書（１つ以上）４１０の取り消しは、データネットワークインシデントに基づき得る。管理システム５１０は、プロキシデバイス１２０の証明書リストを変えるように構成され得、ここにおいて、証明書リストを変えることは、データネットワークインシデントに基づき得る。

【００６２】

プロキシデバイス１２０は、デジタル証明書（１つ以上）４１０のうちの１つ以上を記憶するように構成され得る。プロキシデバイス１２０は、デジタル証明書サーバ４００に１つ以上のデジタル証明書（１つ以上）４１０を送信するように更に構成され得、ここにおいて、デジタル証明書サーバ４００は、デジタル証明書（１つ以上）４１０を認証するように構成され得る。プロキシデバイス１２０は、プロキシデバイス１２０を介してデータネットワーク１１０に結合されたリソース１３０からの通信試行に基づいてデジタル証明書４１０を送信するように構成され得る。

【００６３】

プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０は、識別装置３００を備え得、それは、受信機３１０を備え得る。管理システム５１０は、識別装置３００に基づいて、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の識別及び／又は位置推定を実行するように構成され得る。管理システム５１０は、プロキシデバイス１２０及び／又はリソース（１つ以上）１３０に位置要求を送るように構成され得る。加えて、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０は、通信システム１００及び／又は管理システム５１０に位置を送信するように構成され得る。故に、プロキシデバイス１２０及び／又はリソース１３０の位置が地理的に又はデータネットワーク１１０に関して変更された場合、通信システム１０

０及び／又は管理システム５１０は、変更を登録し得る。管理システム５１０は、プロキシデバイス（１つ以上）１２０及びリソース（１つ以上）１３０の識別及び／又は位置推定の分析、プロキシデバイス（１つ以上）１２０及びリソース（１つ以上）１３０の識別及び／又は位置推定の追跡、及び／又はプロキシデバイス（１つ以上）１２０及びリソース（１つ以上）１３０の識別及び／又は位置推定の制御を実行するように更に構成され得る。

【００６４】

更に、管理システム５１０は、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の位置のインジケーションを受信するように構成され得る。管理システム５１０は、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の位置のインジケーションを追跡するように構成され得る。故に、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の位置のインジケーションが変化すると、管理システム５１０は、この変化を追跡するように構成され得る。位置のインジケーションの変化は、１つ以上のデータネットワークインシデントによって構成され得る。管理システム５１０は、位置のインジケーションの変化に基づいて通信を制御するように構成され得る。更に、管理システム５１０は、識別装置３００の識別に基づいて識別データを生成するように構成され得る。管理システム５１０は、生成された識別データに基づいて、プロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の挙動を識別するように構成され得る。「挙動」という用語は、データネットワーク１１０、プロキシデバイス（１つ以上）１２０、リソース（１つ以上）１３０、及び／又はユーザデバイス（１つ以上）１４０の接続、切断、ユーザ識別（user identity）、及び／又は結合／接合を意味する。管理システム５１０は、該データを使用して、経時的にプロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０の挙動を追跡及び／又はマッピングするように構成され得る。

【００６５】

当業者は、本発明が、上述された好ましい実施形態に決して限定されないことを理解する。それどころか、添付された特許請求の範囲内において多くの変更及び変形が可能である。例えば、任意のプロキシデバイス（１つ以上）１２０及び／又はリソース（１つ以上）１３０が、識別装置３００を備え得る。更に、各識別装置３００は、受信機３１０を備え得る。各プロキシデバイス１２０は、第１の通信ポート２１０及び／又は第２の通信ポート２２０を備え得る。更に、プロキシデバイス（１つ以上）１２０及び／又は管理システム５１０は、データネットワーク１１０を介してデジタル証明書サーバ４００に通信可能に結合され得る。加えて、管理システム５１０は、１つ以上の証明書デバイス４２０を備え得る。言い換えれば、リソース（１つ以上）１３０、プロキシデバイス（１つ以上）１２０、及び／又はユーザデバイス（１つ以上）１４０は、証明書デバイス４２０に結合され得る。

【００６６】

本発明の更なる目的、特徴、及び利点は、以下の詳細な開示、図面、及び添付された特許請求の範囲を参酌すると明らかになるであろう。当業者は、本発明の異なる特徴が、以下に説明される実施形態以外の実施形態を作り出すために組み合わされることができることを理解するであろう。

［実施形態の項目別リスト］

【００６７】

［項目１］

通信信号を受信及び送信するための通信システム（１００）であって、

データネットワーク（１１０）と、

前記データネットワークに結合された少なくとも１つのプロキシデバイス（１２０）と、ここにおいて、前記少なくとも１つのプロキシデバイスは、デジタル証明書認証のために構成される、

少なくとも１つのリソース（１３０）と

を備え、前記少なくとも１つのプロキシデバイスのうちの各プロキシデバイスは、前記少なくとも１つのリソースのうちのそれぞれのリソースに結合され、前記少なくとも１つのリソースは、前記少なくとも１つのプロキシデバイスを介して前記データネットワークに通信可能に結合され、前記少なくとも１つのプロキシデバイスは、デジタル証明書認証に基づいて、前記データネットワークと前記少なくとも１つのリソースとの間の通信を制御するように構成される、通信システム。

［項目２］

前記少なくとも１つのプロキシデバイスは、少なくとも１つのデジタル証明書を記憶するように構成される、項目１に記載の通信システム。

［項目３］

前記少なくとも１つのプロキシデバイスは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵のうちの少なくとも１つを生成するように構成される、項目１又は２に記載の通信システム。

［項目４］

前記少なくとも１つのプロキシデバイスは、証明書デバイス、パスワード、ＩＰアドレス、ＩＰポート、及びＭＡＣアドレスのうちの少なくとも１つに基づいて、前記データネットワークと前記少なくとも１つのリソースとの間の通信を制御するように更に構成される、項目１～３のうちのいずれか一項に記載の通信システム。

［項目５］

前記少なくとも１つのプロキシデバイスは、前記少なくとも１つのリソースに結合された第１の通信ポート（２１０）と、前記データネットワークに結合された第２の通信ポート（２２０）とを備える、項目１～４のうちのいずれか一項に記載の通信システム。

［項目６］

前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つは、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの識別情報及び位置のうちの少なくとも１つを示すように構成された識別装置（３００）を備える、項目１～５のうちのいずれか一項に記載の通信システム。

［項目７］

前記識別装置は、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの位置を受信するための受信機（３１０）を備える、項目６に記載の通信システム。

［項目８］

通信装置（５００）であって、

項目１～７のうちのいずれか一項に記載の通信システムと、

前記少なくとも１つのプロキシデバイスに結合された管理システム（５１０）と、ここにおいて、前記管理システムは、前記少なくとも１つのプロキシデバイスと前記管理システムとの間でデジタル証明書認証データを通信するように構成される、

を備える、通信装置。

［項目９］

項目３に記載の前記通信システムを更に備え、前記管理システムは、前記少なくとも１つの公開鍵及び前記少なくとも１つの私有鍵のうちの少なくとも１つを記憶するように構成される、項目８に記載の通信装置。

［項目１０］

前記管理システムは、少なくとも１つの公開鍵及び少なくとも１つの私有鍵を生成するように構成され、前記少なくとも１つの公開鍵及び前記少なくとも１つの私有鍵のうちの少なくとも１つに基づいて、少なくとも１つのデジタル証明書を生成するように更に構成される、項目８に記載の通信装置。

［項目１１］

項目６又は７に記載の前記通信システムを更に備え、前記管理システムは、前記識別装

置に基づいて、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの識別及び位置推定のうちの少なくとも１つを実行するように構成される、項目８に記載の通信装置。

［項目１２］

前記管理システムは、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの分析と、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの追跡と、前記少なくとも１つのプロキシデバイス及び前記少なくとも１つのリソースのうちの少なくとも１つの前記識別及び前記位置推定のうちの少なくとも１つの制御とのうちの少なくとも１つを実行するように更に構成される、項目１１に記載の通信装置。

［項目１３］

前記管理システム及び前記少なくとも１つのプロキシデバイスのうちの少なくとも１つは、前記データネットワークと前記少なくとも１つのプロキシデバイスとの間のデータ通信を登録するように構成される、項目８～１２のうちのいずれか一項に記載の通信装置。

［項目１４］

登録されたデータ通信は、タイムスタンプ、前記少なくとも１つのリソースから前記データネットワークへのデータ、前記データネットワークから前記少なくとも１つのリソースへのデータ、データ通信の送信機、データ通信の受信機、前記データ通信の量、前記データ通信のタイプ、データ通信タイムアウトの数、データ通信試行の数、及び証明書データのうちの少なくとも１つを備える、項目１３に記載の通信装置。

［項目１５］

前記管理システム及び前記少なくとも１つのプロキシデバイスのうちの少なくとも１つは、前記登録されたデータ通信に基づいて、前記データネットワークと前記少なくとも１つのプロキシデバイスとの間の前記通信を制御するように更に構成される、項目１３又は１４に記載の通信装置。

【図１】

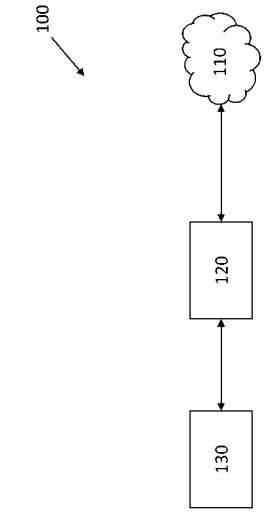

Fig. 1

【図２】

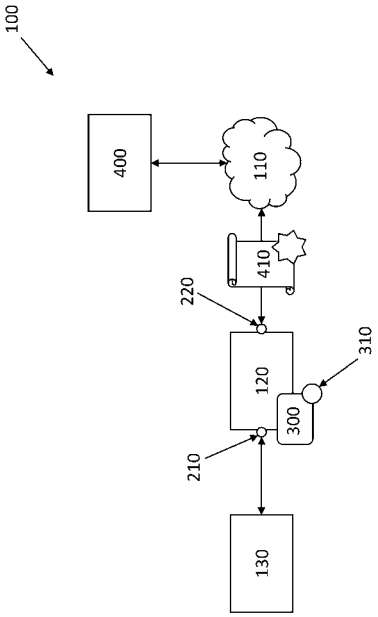

Fig. 2

【図３】

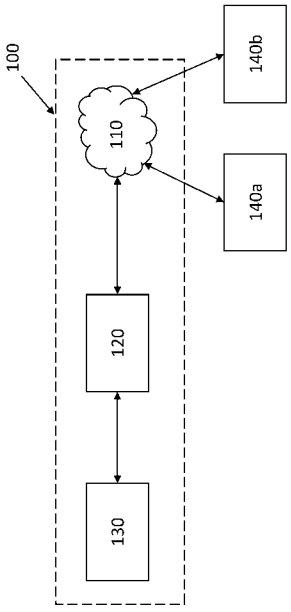

Fig. 3

【図４】

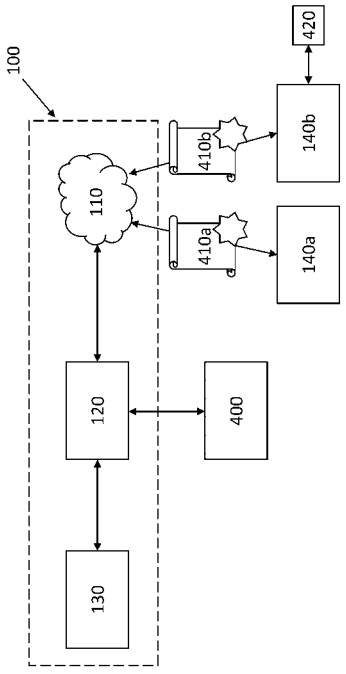

Fig. 4

【図５】

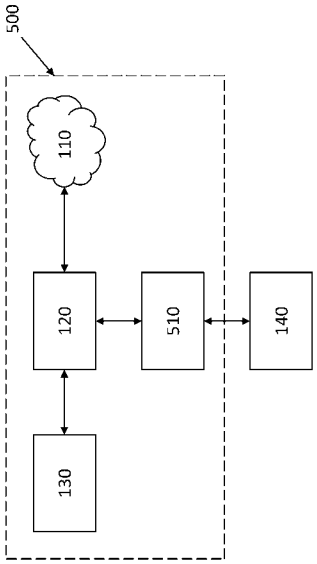

Fig. 5

【図６】

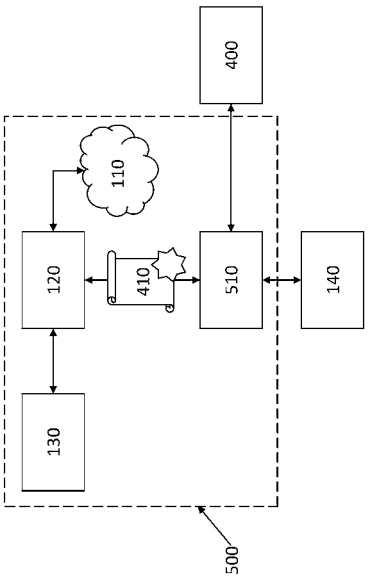

Fig. 6

フロントページの続き

(74)代理人 100199565
弁理士 飯野 茂
(74)代理人 100219542
弁理士 大宅 郁治
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100162570
弁理士 金子 早苗
(72)発明者 マーティン・エリクソン
スウェーデン国、１６９ ７３ ソルナ、ポモナガタン ５
(72)発明者 ジェンズ・アルム
スウェーデン国、１３５ ５４ タイレソ、リルジェグランド ２

【外国語明細書】
2021069113000001.pdf