

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5622011号

(P5622011)

(45) 発行日 平成26年11月12日 (2014.11.12)

(24) 登録日 平成26年10月3日 (2014.10.3)

(51) Int.Cl.

F I

H O 4 L 12/46 (2006.01)

H O 4 L 12/46 E

H O 4 L 12/66 (2006.01)

H O 4 L 12/66 B

H O 4 W 12/08 (2009.01)

H O 4 W 12/08

H O 4 W 76/02 (2009.01)

H O 4 W 76/02

H O 4 W 84/12 (2009.01)

H O 4 W 84/12

請求項の数 19 外国語出願 (全 26 頁)

(21) 出願番号 特願2013-184326 (P2013-184326)
 (22) 出願日 平成25年9月5日 (2013.9.5)
 (65) 公開番号 特開2014-53897 (P2014-53897A)
 (43) 公開日 平成26年3月20日 (2014.3.20)
 審査請求日 平成25年11月5日 (2013.11.5)
 (31) 優先権主張番号 13/603,545
 (32) 優先日 平成24年9月5日 (2012.9.5)
 (33) 優先権主張国 米国 (US)

(73) 特許権者 000002185
 ソニー株式会社
 東京都港区港南1丁目7番1号
 (74) 代理人 100092093
 弁理士 辻居 幸一
 (74) 代理人 100082005
 弁理士 熊倉 禎男
 (74) 代理人 100067013
 弁理士 大塚 文昭
 (74) 代理人 100109070
 弁理士 須田 洋之
 (74) 代理人 100109335
 弁理士 上杉 浩
 (74) 代理人 100158551
 弁理士 山崎 貴明

最終頁に続く

(54) 【発明の名称】 広告現場において電光サインを動作するように構成するためのシステム及び方法

(57) 【特許請求の範囲】

【請求項1】

少なくとも1つのディスプレイと、
 前記ディスプレイを制御する少なくとも1つのプロセッサと、
 制御サーバの予めプログラムされたネットワークアドレスを記憶し、前記プロセッサがアクセス可能な少なくとも1つのコンピュータ可読記憶媒体と、
 を備えた電光サインであって、前記少なくとも1つの媒体には命令がプログラムされ、該命令は、前記プロセッサに対し、

複数の無線ルータを全て共通のサブネット上に有する広告現場における最初の通電時に、前記広告現場の無線ルータに自動的に接続させて前記共通のサブネットに参加させ、
 前記共通のサブネットに参加した後に、前記制御サーバの前記ネットワークアドレスを用いて前記制御サーバにアクセスさせ、

前記電光サインを機械的に設置した後、前記電光サインを動作するように構成する上で有用な構成情報を前記制御サーバから受け取らせ、

前記共通のサブネットに参加した後に、前記サブネットを通じてインターネットにアクセスできるかどうかを判断させ、前記サブネットを通じてインターネットにアクセスできないという判断に回答して、前記予めプログラムされたアドレスを用いて前記制御サーバとのセキュアな接続を確立させ、前記制御サーバから前記サブネット上のローカルサーバに関する情報を取得して、前記電光サインを前記サブネット上の前記ローカルサーバと通信させ、前記サブネットを通じてインターネットにアクセスできないという判断に回答して

10

20

、前記サブネット上の前記ローカルサーバとの通信を確立させることを特徴とする電光サイン。

【請求項 2】

前記サブネットは、インターネットアクセスを提供し、前記予めプログラムされたネットワークアドレスは、インターネット上の制御サーバのインターネットプロトコル（IP）アドレスである、
ことを特徴とする請求項 1 に記載の電光サイン。

【請求項 3】

前記サブネットは、インターネットアクセスを提供せず、前記予めプログラムされたネットワークアドレスは、ローカルサブネット上の制御サーバのアドレスである、
ことを特徴とする請求項 1 に記載の電光サイン。

10

【請求項 4】

前記サブネット上の前記制御サーバは、インターネットと通信しない、
ことを特徴とする請求項 3 に記載の電光サイン。

【請求項 5】

前記プロセッサは、前記制御サーバからソフトウェアアップデートに関する情報を受け取るようにも構成される、
ことを特徴とする請求項 1 に記載の電光サイン。

【請求項 6】

前記構成情報は、インターネットプロトコル（IP）アドレス及びサブネットアドレスを含む、
ことを特徴とする請求項 1 に記載の電光サイン。

20

【請求項 7】

複数のノードを含むサブネットと、
少なくとも 1 つのディスプレイと、該ディスプレイを制御する少なくとも 1 つのプロセッサとを含み、前記サブネット内でノードを確立する少なくとも 1 つの電光サインと、
前記サブネットを介して前記電光サインの前記プロセッサと通信し、前記電光サインと少なくとも 1 つの構成メッセージを交換する少なくとも 1 つのプロセッサを含む、前記サブネット内でノードを確立する少なくとも 1 つの制御サーバと、
を備えたシステムであって、

30

前記少なくとも 1 つの構成メッセージは、広告現場における前記電光サインの最初の通電時に、前記電光サインを動作するように構成するために有用であり、

前記サブネット内のノードのプロセッサは、応答メッセージの受け取りに少なくとも基づいて、前記少なくとも 1 つの構成メッセージが前記サブネット内の別のノードに正常に送信されたと判断し、

前記構成メッセージを送信した前記ノードの前記プロセッサは、応答メッセージを受け取ることなくタイマが時間切れした時点で、前記構成メッセージの送信先である前記ノードにより前記構成メッセージが正常に受け取られなかったと判断し、

前記ディスプレイを制御する前記少なくとも 1 つのプロセッサは、

前記サブネットに参加した後に、前記サブネットを通じてインターネットにアクセスできるかどうかを判断し、前記サブネットを通じてインターネットにアクセスできるという判断に応答して、前記予めプログラムされたアドレスを用いて前記制御サーバとのセキュアな接続を確立し、前記制御サーバから前記サブネット上のローカルサーバに関する情報を取得して、前記電光サインを前記サブネット上の前記ローカルサーバと通信し、前記サブネットを通じてインターネットにアクセスできないという判断に応答して、前記サブネット上の前記ローカルサーバとの通信を確立することを特徴とするシステム。

40

【請求項 8】

前記タイマの時間切れを表す時間は、少なくとも $2t + p$ により確立され、式中の「 t 」は、前記メッセージを送信する前記ノードから該メッセージの送信先である前記ノードにメッセージが送信されるための最大時間を定義し、「 p 」は、前記メッセージの送信先

50

である前記ノードによって前記構成メッセージが処理されるための最大時間である、
ことを特徴とする請求項7に記載のシステム。

【請求項9】

前記構成メッセージを送信した前記ノードは、該構成メッセージを送信した該ノードによるタイムアウト前に、前記タイマのそれぞれの時間切れ後に前記構成メッセージを前記別のノードに「r」回再送し、前記構成メッセージを送信した前記ノードによるタイムアウト前の最大時間は、 $r(2t + p)$ により確立される、
ことを特徴とする請求項8に記載のシステム。

【請求項10】

前記構成メッセージは、所定の回数繰り返されるサブネット固有のセキュリティフィールドを含む、
ことを特徴とする請求項7に記載のシステム。

10

【請求項11】

前記所定の回数は、前記電光サインが最初に通电されて前記サブネットを介して通信する前に、前記制御サーバ及び電光サインの両方に知られている、
ことを特徴とする請求項10に記載のシステム。

【請求項12】

前記セキュリティフィールドは、サブネット固有の秘密鍵を用いてアルゴリズムから導出される、
ことを特徴とする請求項10に記載のシステム。

20

【請求項13】

前記秘密鍵は、前記電光サインが最初の通电時に、前記電光サインの前記プロセッサが前記サブネットを介して通信するよう利用できるように、前記電光サインが最初に通电されて前記サブネットを介して通信する前に前記電光サインのコンピュータ可読記憶媒体に記憶される、
ことを特徴とする請求項12に記載のシステム。

【請求項14】

前記秘密鍵は、前記サブネットを介した送信以外の通信手段により、前記制御サーバ及び電光サインの両方に提供される、
ことを特徴とする請求項12に記載のシステム。

30

【請求項15】

前記構成メッセージは、前記サブネット上のサーバを発見する発見メッセージであり、前記アルゴリズムは、前記サブネットのE S S I Dも使用する、
ことを特徴とする請求項10に記載のシステム。

【請求項16】

前記構成メッセージは、前記サブネット上のサーバを発見する発見メッセージへのサーバ応答メッセージであり、前記アルゴリズムは、前記サーバ応答メッセージを送信する前記サーバの前記M A Cアドレスも使用する、
ことを特徴とする請求項10に記載のシステム。

【請求項17】

前記セキュリティフィールドは、前記メッセージのテイル内に存在する、
ことを特徴とする請求項10に記載のシステム。

40

【請求項18】

サブネット上に少なくとも1つの無線ルータを有する広告現場におけるデジタルサインの最初の通电時に、該デジタルサインを前記広告現場の無線ルータに自動的に接続して前記サブネットに参加させるステップと、

ローカルサブネット上又はインターネット上の制御サーバにアクセスするステップと、
前記デジタルサインを動作するように構成する上で有用な少なくとも1つの構成パケットを前記制御サーバから受け取るステップと、
を含む方法であって、

50

前記構成パケットは、該パケットのヘッダ又はテイル内に、サブネット固有の秘密鍵を用いてアルゴリズムから導出されたサブネット固有のセキュリティフィールドを含み、

方法は、

前記サブネットに参加した後に、前記サブネットを通じてインターネットにアクセスできるかどうかを判断するステップと、

前記サブネットを通じてインターネットにアクセスできるという判断に応答して、前記予めプログラムされたアドレスを用いて前記制御サーバとのセキュアな接続を確立するステップと、

前記制御サーバから前記サブネット上のローカルサーバに関する情報を取得して、前記電光サインを前記サブネット上の前記ローカルサーバと通信するステップと、

前記サブネットを通じてインターネットにアクセスできないという判断に応答して、前記サブネット上の前記ローカルサーバとの通信を確立するステップとを含む、方法。

10

【請求項 19】

前記方法は、少なくとも 1つのパケットを受け取った後に、接続メッセージを含む少なくとも 1つのパケットを前記制御サーバに送信し、前記制御サーバを通信から接続するステップを含み、切断されるパケットは、前記サブネット固有のセキュリティフィールドを含む、

ことを特徴とする請求項 18 に記載の方法。

【発明の詳細な説明】

【技術分野】

20

【0001】

本出願は、一般に広告現場において電光サインを動作するように容易かつ自動的に構成することに関する。

【背景技術】

【0002】

近年、電光サインシステムの使用が増加してきた。これらの電光サイン及び関連するシステムは、広告及び情報の公共表示などの多くの目的に有用である。これらのシステムの多くでは、テレビ（TV）を電光サインとして使用する。

【発明の概要】

【発明が解決しようとする課題】

30

【0003】

しかしながら、本原理は、これらの電光サインを組み込むこと、及びこれらを電光サインネットワークに参加させることにより遠隔的に制御されるようにすることは困難かつ多大な労力を要することが明らかになってきたと認識する。例えば、技術者が容易に届かない高さに電子ディスプレイが配置され、電光サインのソフトウェアの制御及びアップデートが困難になることがある。

【課題を解決するための手段】

【0004】

従って、本原理は、電光サインの配置、制御及びアップデートに必要な、各電光サインにおける直接的、物理的活動を最低限に抑えるべきであると認識する。本原理は、電光サインシステムが、ネットワーク攻撃及びハッキングなどから守られるように適切なセキュリティを有する必要性も認識する。

40

【0005】

従って、電光サインが、少なくとも 1つのディスプレイと、このディスプレイを制御する少なくとも 1つのプロセッサと、制御サーバの予めプログラムされたネットワークアドレスを記憶する、プロセッサがアクセス可能な少なくとも 1つのコンピュータ可読記憶媒体とを含む。この媒体には、複数の無線ルータを全て共通のサブネット上に有する広告現場における最初の通電時に、プロセッサを広告現場の無線ルータに自動的に接続させて共通のサブネットに参加させるための命令がプログラムされる。この命令は、プロセッサを、共通のサブネットに参加した後に制御サーバのネットワークアドレスを用いてサーバに

50

もアクセスさせる。また、この命令は、技術者が機械の設置後に電光サインに物理的にアクセスしてサインを動作するようにさらに構成する必要がないように、サインを動作するように構成する上で有用な構成情報をプロセッサが制御サーバから受け取るようにする。

【0006】

いくつかの実施形態では、サブネットがインターネットアクセスを提供し、予めプログラムされたネットワークアドレスをインターネット上の制御サーバのインターネットプロトコル（IP）アドレスとすることができる。他の実施形態では、サブネットがインターネットアクセスを提供せず、従って予めプログラムされたネットワークアドレスをサブネット上の制御サーバのアドレスとすることができる。従って、制御サーバは、常にインターネットを介して通信しなくてもよい。

10

【0007】

従って、いくつかの実施形態では、プロセッサを、共通のサブネットに参加した後に、このサブネットを通じてインターネットにアクセスできるかどうかを判断するように構成することができる。プロセッサは、サブネットを通じてインターネットにアクセスできるという判断に応答して、予めプログラムされたアドレスを用いて制御サーバとのセキュアな接続を確立し、そこからサブネット上のローカルサーバに関する情報を取得して、このサブネット上のローカルサーバと通信するようにサインを構成することができる。一方、プロセッサは、サブネットを通じてインターネットにアクセスできないという判断に応答して、サブネット上のローカルサーバとの通信を確立することができる。

【0008】

20

また、必要に応じて、プロセッサを、ソフトウェアアップデートに関する情報を制御サーバから受け取るように構成することもできる。また、必要に応じて、構成情報は、インターネットプロトコル（IP）アドレス及びサブネットアドレスを含むことができる。

【0009】

別の態様では、システムが、複数のノードを含むサブネットを含む。システムは、ディスプレイ及びこのディスプレイを制御するプロセッサを含む少なくとも1つの電光サインも含む。従って、電光サインがサブネット内でノードを確立すると理解されたい。また、システムは、少なくとも1つの制御サーバを含み、この制御サーバ自体が、サブネットを介して電光サインのプロセッサと通信して電光サインと少なくとも1つの構成メッセージを交換するプロセッサを含む。従って、制御サーバもサブネット内でノードを確立する。少なくとも1つの構成メッセージは、広告現場における電光サインの最初の通電時に電光サインを動作するように構成するために有用であると考えられる。さらに、サブネット内のノードのプロセッサは、少なくとも応答メッセージの受け取りに基づいて、構成メッセージのうちの1つがサブネット内の別のノードに正常に送信されたと判断すると理解されたい。また、構成メッセージを送信したノードのプロセッサは、応答メッセージを受け取らずにタイマが時間切れした時点で、送信先のノードが構成メッセージを正常に受け取らなかったと判断する。

30

【0010】

さらに別の態様では、方法が、少なくとも1つの無線ルータをサブネット上に有する広告現場におけるデジタルサインの最初の通電時に、デジタルサインを広告現場の無線ルータに接続してサブネットに参加させるステップを含む。この方法は、サブネット上の制御サーバにアクセスして、サインを動作するように構成するために有用な少なくとも1つの構成パケットを制御サーバから受け取るステップをさらに含む。構成パケットは、そのパケットのヘッダ又はテイルに、サブネット固有の秘密鍵を使用するアルゴリズムから導出されたサブネット固有のセキュリティフィールドを含むと理解される。

40

【0011】

同じ参照数字が同じ部分を示す添付図面を参照することにより、本発明の詳細を、その構造及び動作の両方に関して最も良く理解することができる。

【図面の簡単な説明】

【0012】

50

【図 1】本原理による非限定的なシステム例のブロック図である。

【図 2】少なくとも 1 つのサブネットを含む例示的なネットワークを示す図である。

【図 3】少なくとも 1 つのサブネットを含む例示的なネットワークを示す図である。

【図 4】少なくとも 1 つのサブネットを含む例示的なネットワークを示す図である。

【図 5】電光サインのプロセッサにより実行される、ローカル制御サーバ又はインターネット制御サーバに接続するためのロジック例のフローチャートである。

【図 6】本原理による、1 つのノードから送信されたメッセージ及びパケットの送信及び処理時間のグラフィック表現である。

【図 7】本原理による、ネットワーク及び／又はサブネットを介して送信される例示的なメッセージの説明図である。

10

【図 8】本原理による、サーバの発見及び認証処理の例示的な説明図である。

【図 9】本原理による、サーバの発見及び認証処理の例示的な説明図である。

【図 10】本原理による、サーバの発見及び認証処理の例示的な説明図である。

【図 11】本原理による、ネットワーク／サブネットに参加するノードにより実行されるロジック例のフローチャートである。

【図 12】電光サインなどのノードがネットワーク及び／又はサブネットに参加しようとする際の、制御サーバにより実行される例示的なフローチャートである。

【発明を実施するための形態】

【0013】

まず、図 1 に示す例示的な実施形態を参照すると、概略的に 10 で示す例示的なサブネットワーク（「サブネット」）を示している。システム 10 は、少なくとも 1 つの電光サイン 12、少なくとも 1 つのルータ 14、及び少なくとも 1 つのサーバ 16 を含む。電光サイン 12 は、一例として、高解像度テレビ（TV）などのテレビとすることができる。しかしながら、以下に限定するわけではないが、インターネット対応 TV、スマート TV、大画面 TV、「ジャンボトロン（jumbotrons）」、コンピュータモニタ、又はデジタルディスプレイ、プラズマディスプレイ、LCD ディスプレイ、LED ディスプレイ、OLED ディスプレイ、ELD ディスプレイ、プロジェクタ及びプロジェクタディスプレイ、デジタルポスター、（例えば、表面上に可動的に装着された）タブレットコンピュータ、（例えば、表面上に可動的に装着可能なスマートフォンなどの）タッチスクリーンディスプレイ、（例えば、人が着用する）標識ベスト、セグメントディスプレイ、2 次元及び 3 次元ディスプレイの両方、頭部装着型ディスプレイ、ブラウン管ディスプレイなどの他のあらゆるタイプの適当なディスプレイなどの電光サイン（モバイル、屋内及び屋外）にも本原理を適用できると理解されたい。従って、いくつかの実施形態では、電光サイン 12 を、Sony 社製の Sony Bravia 高繊細度テレビとすることができる。

20

30

【0014】

これに関わらず、電光サイン 12 は、情報及び広告などを視聴者に提示するためのディスプレイ 18 を含み、従ってこのような目的でユーザインターフェイス、ビデオ、オーディオ及び／又は画像を提示することができる。電光サイン 12 は、ディスプレイ 18 を制御する少なくとも 1 つのプロセッサ 20、ディスクベースのストレージ又はソリッドステートストレージなどの少なくとも 1 つの有形コンピュータ可読記憶媒体 22、少なくとも 1 つの TV チューナ 24、及び任意にセットトップボックス、DVD プレーヤ又はビデオゲーム機などの、電光サイン 12 に電氣的に接続されたその他の装置と HDMI 接続などを介して通信するための少なくとも 1 つのオーディオ／ビデオインターフェイス 26 も含む。電光サイン 12 は、本原理に従ってインターネット及び／又はサブネットなどのネットワークを介して通信するための、例えば有線又は無線モデム又はルータ、或いは無線回線送受信機などの他の適当なインターフェイスとすることができる少なくとも 1 つのネットワークインターフェイス 28 も含む。従って、本原理によれば、ネットワークインターフェイス 28 は、ルータ 14 及びサーバ 16 への接続性を提供し、ルータ 14 及びサーバ 16 も、このような接続性を容易にするための（簡潔に説明すれば）それぞれのネットワ

40

50

ークインターフェイスを有すると理解されたい。

【0015】

上記に加え、電光サイン12は、オーディオ信号を出力するための1又はそれ以上のスピーカ30を含むこともできる。従って、本原理によれば、電光サイン12は、サブネットを介して情報を受け取ることに加え、インターネット、ケーブルTVプロバイダ及び衛星TVプロバイダなどのソースからオーディオビデオ番組及び／又はその他のコンテンツを受け取り、これによりプロセッサ20の制御下でディスプレイ18及びスピーカ20上にコンテンツを提示できると理解することもできる。さらに、いくつかの実施形態では、プロセッサ20へのコマンドを、サブネットを介してだけでなく、マウス、キーボード、キーパッド、リモコン装置、タッチパッド、タッチスクリーンなどの1又はそれ以上の入力装置32を介して受け取ることもできる。例示的な電光サイン12上には、例えば、マーケティング目的、広告効果の分析及び顔認識技術を用いた視聴者の反応分析のために電光サインの視聴者の写真／画像及びビデオを収集するための、熱探知カメラ、ウェブカムなどのデジタルカメラ、及び／又はTVに内蔵されてプロセッサ20により制御可能なカメラなどとして行うことができる少なくとも1つのカメラ34も示している。

10

【0016】

上述したように、図1にはルータ14も示している。ルータ14は、有線及び／又は無線ルータとすることができ、少なくとも1つのプロセッサ36、及びディスクベースのストレージ又はソリッドステートストレージなどの少なくとも1つの有形コンピュータ可読記憶媒体38を含む。ルータ14は、ネットワークインターフェイスなどの少なくとも1つのインターフェイス40も含む。少なくとも1つのインターフェイス40は、インターネット、WAN、LANなどのネットワーク及びサブネットへの接続性を提供し、ルータ14が本原理に従ってプロセッサ36の制御下でネットワーク及び／又はサブネットを介してトラフィックを制御及び／又はルーティングできるようにし、実際に少なくとも部分的にネットワーク及び／又はサブネットを確立できると理解されたい。

20

【0017】

上述したように、図1には少なくとも1つのサーバ16も示している。サーバ16は、少なくとも1つのプロセッサ42、及びディスクベースのストレージ又はソリッドステートストレージなどの少なくとも1つの有形コンピュータ可読記憶媒体44を含む。上述したように、サーバ16は、本原理に従ってインターネット及び／又はサブネットなどのネットワークを介して通信するための、例えば有線又は無線モデム又はルータ、或いは無線回線送受信機などの他の適当なインターフェイスとすることができる少なくとも1つのネットワークインターフェイス46を含む。従って、ネットワークインターフェイス46は、プロセッサ42の制御下で、それぞれのインターフェイス28及び40などを通じてネットワーク及び／又はサブネットを経由する、ルータ14を介した電光サイン12との通信を可能にする。従って、電光サイン12、ルータ14及びサーバ16は、本原理によるネットワーク及び／又はサブネットのノードを確立する。

30

【0018】

次に図2を参照すると、少なくとも1つのサブネットを含む例示的なネットワーク50を示している。ネットワーク50は、Sony社により製造及び／又は制御される専用Sonyサーバなどとして行うことができる少なくとも1つのインターネットサーバ52を含む。インターネットサーバ52は、インターネット54を通じネットワーク50を介して通信する。

40

【0019】

図2には、複数のルータも示している。このように、ルータ200、ルータ202、ルータ204及びルータ206を示しているが、ネットワーク50にはこれよりも多くの又は少ないルータを含めることもできると理解されたい。ルータ200、202、204及び206は、有線及び／又は無線ルータとすることができる。なお、ルータ200は、インターネット54に接続された形で示されており、従ってルータ202、204及び206を含むネットワーク50上の他のノードにインターネット接続をルーティングすると

50

もに、図2に示すサイン56、58、60及び62などの複数の電光サインにインターネット接続をルーティングすることもできる。換言すれば、ルータ200は、サブネットがインターネットにアクセスできるようにするゲートウェイルータとすることができる。

【0020】

図2にはローカル制御サーバ64も示しており、例示的な実施形態では、このサーバは、実装によってはインターネットに直接又は全く接続できないという点で、これ自体はインターネットサーバではない。さらに、ローカル制御サーバ64は、電光サイン56、58、60及び62が存在する現場又はその近くに位置するサーバとすることができる。

【0021】

図2から理解できるように、無線ルータ206は、電光サイン56、58、60、62、並びにルータ200、202、204及び206から少なくとも構成された共通のサブネット66を少なくとも部分的に定める。例示的な実施形態では、共通のサブネット66がサーバ64を含むこともできる。しかしながら、サブネット66、従ってルータ206、並びに電光サイン56、58、60及び62は、より小さな又は大きなサブネットの一部とすること、ネットワーク50の一部とすることもでき、図2に示すルータの1又はそれ以上などを通じ、本原理によるネットワーク50を介して通信できると理解されたい。

【0022】

さらに、電光サイン56、58、60及び62は、機能及び構成が上述の電子ディスプレイ12と実質的に同様であり、ルータ200、202、204及び206は、機能及び構成が上述のルータ14と実質的に同様であり、サーバ52及び64は、機能及び構成が上述のサーバ16と実質的に同様であると理解されたい。さらに、サーバ52及び64、電光サイン56、58、60及び62、並びにルータ200、202、204及び206の各々は、本原理によるそれぞれのネットワーク及び／又はサブネットノードを確立することができる。さらに、これらのノードを互いに、従ってWi-Fi接続、イーサネット接続、1又はそれ以上のケーブル接続などのいずれかの好適な手段を介してネットワーク50に接続することもできる。

【0023】

ここで図3を参照すると、上述したネットワーク50を再び示している。図3から理解できるように、電光サイン62が、ネットワーク及び／又は上述のサブネット66などの少なくとも1つの共通のサブネットに参加するために、無線ルータ206に自動的に接続しようとして試みている様子を示している。図示の例示的な実施形態では、電光サイン62が（及びいくつかの実施形態では、ルータ204及び206などの1又はそれ以上のルータも）、電光サイン62が1又はそれ以上の視聴者に広告及び／又はその他のコンテンツを提示する予定の現場に位置すると理解されたい。現場とは、公園、モール、市街道路、オフィスビル、イベントセンターなどの公共の場とすることができる。従って、やはり例示的な実施形態では、電光サイン62が、広告現場における最初の通電（例えば、電源オン）時に、自動接続を開始して少なくとも1つのサブネットに接続し、これに参加する。図3に示すように、電光サイン62は、wireless protected setup (WPS) 技術及びその対応するプッシュボタン制御を使用して無線ルータ206に接続することができるが、他の好適な手段を使用してもよい。

【0024】

図3を続けて参照すると、電光サイン62が、共通のサブネット66に参加した後に、インターネットを介して（サーバ52などの）制御サーバに接続してこれにアクセスし、サーバが本原理による電光サイン62に構成情報、ソフトウェアアップデート及びこれに関連する情報、広告及びその他の情報などを提供できるように、サブネット66がインターネットアクセスを提供するかどうかを判断することを示す矢印70を示している。さらに、構成情報は、ローカルコントローラサーバがさらなる／後続のアップデートのために接続するための詳細（IPなど）を含むことができる。

【0025】

従って、例示的な実施形態では、サイン62上のコンピュータ可読記憶媒体が、制御サ

10

20

30

40

50

サーバに接続してアクセスするために有用な、インターネット制御サーバのネットワークアドレスを記憶し及び／又はこれを予めプログラムされると理解される。なお、「予めプログラムされた」とは、広告現場におけるサイン６２の通電前に記憶媒体にアドレスが記憶されていることを少なくとも意味する。しかしながら、これに加えて又はこれとは別に、サイン６２がインターネット制御サーバ５２にアクセスしようと試みる前などに、サイン６２の通電時にサブネット６６の管理者などがサイン６２にネットワークアドレスを提供しておくこともできる。

【００２６】

これに関わらず、電光サイン６２が、予めプログラムされたネットワークアドレスを用いてインターネット５４を介してサーバ５２に接続しアクセスできると判断した場合、電光サイン６２及びサーバ５２は、少なくともサイン６２を動作するように構成する上で有用な構成情報を交換する。サイン６２及びサーバ５２は、以下でより完全に説明するように、セキュアな接続及び／又はプロトコルを使用して、さらに別の情報に加え、追加のネットワーク及びサブネットアドレス情報（例えば、電光サイン６２、共通のサブネット６６上のローカル制御サーバ６４及びその他のノードのネットワーク及びサブネットアドレス（ＩＰアドレスなど））を交換することもできる。

10

【００２７】

より具体的には、サイン６２は、共通のサブネット６６上のローカルサーバ（ローカル制御サーバ６４など）に関する情報をインターネット制御サーバ５２から取得して、このサブネット６６上のローカルサーバ６４と通信するようにサイン６２を構成することができる。この情報は、ローカル制御サーバ６４のネットワークアドレス及びサブネットアドレスなどを含むことができる。

20

【００２８】

このセキュアな接続は、サイン６２上のプロセッサが、上述の予めプログラムされたアドレスなどを使用して少なくとも部分的に確立できると理解されたい。従って、電光サイン６２を広告現場に機械的に設置した後に、技術者が電光サイン６２に物理的にアクセスしてサイン６２を動作するように構成する必要があるように、サイン６２が使用する構成情報を交換すべきであると理解することができる。

【００２９】

次に図４を参照すると、再びサイン６２、並びにサーバ５２及び６４を含むネットワーク５０を示している。図４には、サイン６２がセキュアな接続を確立し、本原理によるローカル制御サーバ６４にアクセス及び／又は登録しようと試みていることを示す矢印７２も示している。サイン６２は、本明細書に示すように、ローカル制御サーバ６４のネットワーク情報及び／又は少なくとも１つのアドレスをインターネット制御サーバ５２から受け取った後にこれを行うことができる。

30

【００３０】

しかしながら、サイン６２が、サブネット６６がインターネットアクセスを提供しないと判断した場合、或いはたとえインターネットアクセスが提供されたとしてもインターネット制御サーバ５２にアクセスできないと判断した場合、サイン６２上のプロセッサは、サブネット６６上のローカル制御サーバ６４との通信及び／又はこれへのアクセスを確立することができる。

40

【００３１】

従って、サイン６２のコンピュータ可読記憶媒体に予めプログラムされているローカル制御サーバ６４のネットワーク及び／又はサブネットアドレスを使用して通信及び／又はアクセスを確立することができるが、予めプログラムされているアドレスを使用することに加えて又はこの代わりに、当業者が理解できるような他の装置発見原理及び方法を使用することもできる。この場合も、「予めプログラムされた」とは、広告現場におけるサイン６２の通電前に、サイン６２の記憶媒体にネットワーク及び／又はサブネットアドレスが提供されていることを少なくとも意味する。しかしながら、サイン６２がサーバにアクセスしようと試みる前に、サイン６２の通電時にサブネット６６の管理者などがサイン６

50

2にネットワーク及びサブネットアドレスを提供しておくこともできる。これに関わらず、サブネット66によりインターネットアクセスが提供されない場合には、ローカル制御サーバ64はインターネットと通信せずに、サブネット66を介して構成情報、広告コンテンツ及びさらに他の情報をサイン62に提供できると理解することができる。

【0032】

従って、顧客／広告現場におけるルータは、同じサブネット（例えば、255.255.206.0）及びIPの範囲（例えば、192.168.x.y、この場合のxは各ルータのサブネット）上に存在するように構成されると理解されたい。ルータに接続された全てのクライアント（例えば、電光サイン）には、動的ホスト構成プロトコル（DHCP）を介してIPが割り当てられ、これらのクライアントは、メインサブネット（例えば、255.255.206.0）の一部でもある。このようにして、各装置は、サブネット上の、さらにはメインネットワーク上の他の全ての装置を認識することができる。

10

【0033】

上記に加え、本原理は、いくつかの事例では、ある時点で（例えば、構成情報を交換して電光サインソフトウェアをアップデートするためにインターネット制御サーバに接続する前又はインターネット制御サーバに最初に接続した後に）、広告現場がインターネットへのアクセスをブロックしようとすることがあると認識する。このような場合、（展開される電光サインなどの）クライアント装置内のデフォルト構成が、既知のIP（例えば、192.168.200.200）上のローカルコントローラサーバを検索することになる。

20

【0034】

次に、（上述したサイン62などの）電光サインのプロセッサにより実行される、本原理によるローカル制御サーバ又はインターネット制御サーバに接続するためのロジック例のフローチャートである図5を参照する。このロジックは、楕円ブロック80から開始し、視聴者に広告及び／又はその他のコンテンツを提示するために使用される上述したいずれかのような電光サイン（例えば、Sony社製のTV）の電源が、広告現場などにおいてオンになる。次に、ロジックはブロック82に進み、技術者がWPSを使用してサインをローカルルータに接続するための指示を含むダイアログボックス／ユーザインターフェイスを、電光サインのディスプレイ上に提示する。従って、ブロック82において、最も近いローカルルータと接続するようにサインを構成して、ルータ上のWPS接続を容易にするためのWPSボタンを押すように技術者に指示するプロンプトを提示することができる。

30

【0035】

次に、図5のロジックは、菱形判定ブロック84に進み、ローカルルータへのWPS接続が正常に行われたかどうかを判定する。行われていない場合、ロジックはブロック86に進み、電光サインのディスプレイ上にエラーメッセージ及び／又はエラーページを提示し、その後ブロック82に戻ることができる。一方、WPS接続が正常に行われており、従ってサインが本原理による共通のサブネットに参加していた場合、ロジックは、菱形判定ブロック84からブロック86ではなく菱形判定ブロック88に進む。菱形判定ブロック88において、ロジックは、インターネット接続が利用可能であるかどうかを判定する。利用可能である場合、ロジックはブロック90に進み、インターネット接続を使用してインターネット制御サーバへのセキュアな接続を行う。また、ロジックは、ブロック90においてセキュアな接続を行った後に、本原理による、ローカル制御サーバ（例えば、電光サインの広告現場又はその近くのローカル制御サーバ）に接続するための追加情報、アップデート（例えば、電光サインのソフトウェアアップデート）、及び詳細（例えば、ネットワーク及びサブネットアドレス）を収集することができる。

40

【0036】

一方、菱形判定ブロック88において、インターネット接続が利用可能でないと判断した場合、ロジックはブロック90ではなくブロック92に進む。ブロック92において、ロジックは、ローカル制御サーバを発見し及び／又はこれにアクセスするためのセキュア

50

な発見プロトコルを実行する。この実行は、上述したローカル制御サーバの予めプログラムされたアドレスなどを用いて行うことができる。

【0037】

ロジックは、菱形判定ブロック88の後にブロック90に進んだか、それともブロック92に進んだかに関わらず、ブロック90又はブロック92のいずれかからブロック94に進む。ブロック94において、ロジックは、ローカル制御サーバへのセキュアな接続を行ってこれにアクセスし、いくつかの実施形態では、電光サインをこの接続に登録する。

【0038】

従って、この時点で、電光サインがインターネット制御サーバ及びローカル制御サーバの一方又は両方と比較的容易に接続を確立できると理解することができる。本原理は、本明細書に示す開示が、多くの電光サイン及びその他の装置を展開する際に特に有用となり得る一方で、特に多くのサイン／装置を高い位置（例えば、届きにくい場所）に装着／設置する場合に、ユーザ／技術者の関与を最小限しか必要とせず、各電光サイン／装置のセットアップ時間が短縮されると認識している。

【0039】

上述したように、電光サインと制御サーバの間で情報を交換するためには、セキュアな接続／プロトコルを使用することができる。このことが必要な理由は、電光サインと制御サーバが、少なくとも部分的に無線ネットワーク又はサブネットを介して通信し得るからである。本原理は、このような無線媒体は、信頼できないメッセージ配信及びハッキングの影響を受けやすいと認識する。

【0040】

特にメッセージの紛失に関しては、本原理は、以下で簡単に説明するメッセージタイマ及びリトライ機構を採用してあらゆる紛失したメッセージを修復する。従って、ここで図6を参照すると、本原理による、1つのノードから別のノードに送信されるメッセージ及びパケットの送信及び処理時間のグラフィック表現100を示している。

【0041】

まず、サブネット上のノードのプロセッサは、メッセージの送信先であるノードから応答メッセージを受け取った時点で、メッセージ又はパケット（以降、明確にするためにメッセージ及び／又はパケットをメッセージと呼ぶ）が正常に受け取られたと判断できると理解されたい。この応答メッセージは、メッセージの送信先であるノードがメッセージを完全な状態で受け取った旨の受信確認などを含むことができる。しかしながら、最初のメッセージが正常に受け取られなかった場合などには、送信側ノードが応答メッセージを受け取らない場合も考えられる。従って、本原理は、送信側ノードのプロセッサがいつメッセージを再送すべきか（例えば、応答メッセージを受信せずにタイマが時間切れした時点）を判断するためにタイマを使用できると認識する。このようなタイマのパラメータを、図6のグラフィック表現に示す。

【0042】

特に図6に示すものに関して言えば、「t」は、送信側ノードから1「ホップ」だけ離れたノード（例えば、サブネット内の最も近いノード及び／又は一連のノード内の次のノード）にメッセージが届くのに要する最大時間を定義すると理解されたい。また、「p」は、受信側ノードがメッセージを処理するのに必要な時間の上限（例えば、最大値）を定義し、キューイング遅延を含むと理解されたい。送信側ノードは、（ブロードキャスト、構成などを含む）あらゆるメッセージの送信後に、これらのパラメータに基づいてタイマをセットする。従って、タイマ値は、少なくとも（ $2t + p$ ）とすることができる。図6から理解できるように、グラフィック表現100は、ノードAとして示す送信側ノードからノードBとして示す受信側ノードへのメッセージの送信を示す矢印102を含む。

【0043】

図6のグラフィック表現100の各々の側の縦軸は、矢印104が、メッセージがノードBに届くための最大時間である「t」を示し、矢印106が、矢印108で示すノードAへの応答メッセージの返送前にノードBがメッセージを処理するための最大時間である

10

20

30

40

50

「p」を示すように、時間を表すものとして理解されたい。従って、ノードAはノードBにメッセージを送信し、ノードBはノードAにメッセージを返送すると理解することができる。ノードAからメッセージを再送するまでには、ノードBにおける最大メッセージ処理時間を考慮することもできるので、タイマ値は、上述したように少なくとも $(2t + p)$ になり得ると理解することができる。

【0044】

しかしながら、必要に応じて、より大きなタイマ値を選択してプロトコルを「それほど積極的でない」ようにしながら、その正確性を全く落とすことなくレイテンシを増やすこともできる。さらに、ノードAは、タイマの時間切れ前に応答メッセージを受け取らなかった場合、タイマのそれぞれの時間切れ後にメッセージを「r」回送信するように再試行

10

【0045】

次に、広告現場などにおける電光サインの初期セットアップ、認証及び／又は構成中に交換されるメッセージの詳細について説明する。少なくともセキュリティ上の理由で（例えば、リプレーアタックを避けるために）、各メッセージには、送信側ノードのMACアドレスと共にタイムスタンプ及びシーケンス番号をタグ付けすることができる。このことは、複数のノードを通じて送信されるブロードキャストメッセージのブロードキャストストームなどを防ぐ役にも立つ。

20

【0046】

しかしながら、いくつかの実装では、タイムスタンプ情報を使用しないメッセージセキュリティプロトコルを使用してメッセージを送信することができる。このような実装では、チェックサムメッセージの完全性のためにmd5sumを利用し、鍵の生成及び暗号化／復号のためにopensslを利用する。本原理による接続フェーズ中には、2つのノードがそれぞれの公開鍵を交換する。一方のノードは、隣接ノードの公開鍵で一意的なフレーズを暗号化し、メッセージにチェックサムを付加するが、これについては後述する。受信側ノードは、復号してメッセージの完全性を確認し、復号したメッセージの正確性をチェックするが、これについても後述する。

【0047】

以下の説明は、例えば、本原理による、ノード間でメッセージを送信する際に使用できるセキュリティアルゴリズムを提供するものである。従って、全ての送信されるメッセージには、末尾に一意的な「シークレットコード」を付けることができると理解されたい。さらに、このシークレットコードを特定の回数繰り返すことにより、万が一シークレットコードがハッキングされた場合でも、ハッカーは、メッセージ内で「シークレットコード」を何回繰り返すべきかを知らなければ、システムを操作することができない。シークレットコードを特定の回数繰り返すことができるということは、受信側ノードによってメッセージ全体がエラーなく受け取られたことも保証する。

30

【0048】

さらに、本原理は、受信側ノードが、受け取ったメッセージの内容を処理する前に、（例えば、メッセージのヘッダ及び／又はテイルに提供される）完全なシークレットコードが正しく受け取られているかどうかを最初に判断できると認識する。例示的な実装では、特定の広告現場、電光サインのサブネット及び／又はシステムごとにシークレットコードが異なっていて一意であり、これにより一定の分離を提供し、Sony社の電光サインを使用する異なる広告主が運営している可能性のある第2の広告現場におけるセキュリティ違反に起因する第1の広告現場におけるハッキング攻撃を回避する。従って、本原理によれば、広告現場においてノードに通電し、このノードをサブネットに接続する前に、サブネット内の各ノードの記憶媒体に予めシークレットコードをプログラム及び／又はロードしておくことができる。

40

【0049】

50

従って、例えば、広告主は、既に10個のSony社の電光サインを含むサブネットに、さらに4つのSony社の電光サインを追加するように注文することができる。この4つの追加の電光サインには、これらが広告現場に到着してそこで通電される前に、この特定の広告現場用に設計されたシークレットコードをSony社などによって予めプログラムしておくことができる。なお、サブネットアドレス又はサーバアドレスなどのアドレスは、以下の開示による同じ方法で予めプログラムすることができる。しかしながら、必要に応じて、ノードがサブネットに接続／参加しようと試みる前に、広告現場におけるノードの通電時に、サブネットの管理者などがノードにシークレットコードを提供することもできる。

【0050】

従って、例示的な実施形態では、「シークレットコード」を、所定の回数繰り返されるサブネット固有のセキュリティフィールドとすることができる。この所定の回数は、電光サインが最初に通電されてサブネットを介して通信する前に、制御サーバ及び電光サインの両方に既知とすることができる。さらに、このセキュリティフィールドは、電光サインが最初に通電されてサブネットを介して通信する前に、電光サインの最初の通電時に電光サインのプロセッサがサブネットを介して通信するために利用できるように電光サイン上に記憶されているサブネット固有の秘密鍵を用いてアルゴリズムから導出することができる。また、例示的な実施形態では、サブネットを介した送信以外の通信手段により、制御サーバ及び電光サインの両方に秘密鍵を提供することができる。

【0051】

従って、本原理によれば、後述する発見、接続及び／又は認証メッセージの例示的なメッセージコードを以下の通りとすることができる。

```
#define MSG_DISC_REQ 0x60 /* 発見要求メッセージ */
#define MSG_DISC_RSP 0x70 /* 発見応答メッセージ */
#define MSG_CONN_REQ 0x80 /* 接続要求メッセージ */
#define MSG_CONN_CFM 0x90 /* 接続応答メッセージ */
#define MSG_DCONN_REQ 0xA0 /* 接続要求メッセージ */
```

【0052】

また、例示的なメッセージ定数は、以下の通りとすることができる。

```
#define SW_VERSION 1
#define SONY_SECRET_CODE 0x5A /* 追加保護のために
メッセージパケットをパディング */
#define CODE_LENGTH 4 /* 上記コードをパディングすべき回数
*/
```

【0053】

以下の表に、例示的なメッセージの一般的フォーマットを示しており、これらは以下の通りとすることができる。

フィールド 記述子	ソフトウェア	トランザク ション	メッセージ	メッセージ	繰り返され るシークレ ットコード (1バイト)
サイズ (バイト)	1	2	1	メッセージ 長	コード長

【0054】

従って、例示的な電光サインシステムは、メッセージコード及びメッセージ定数を用いてノード間でメッセージを交換及び／又は送信して、例示的なメッセージ110の説明図である図7に示す例示的なメッセージなどのメッセージを送信することができる。メッセージ110は、メッセージヘッダ112、メッセージ本体114及びメッセージテイル1

16を含む。メッセージヘッダ112は、メッセージ長118、ソフトウェアバージョン120、メッセージシーケンス122、メッセージタイムスタンプ124及びメッセージタイプ126などに関する情報を含む。メッセージ本体114は、一意のパスフレーズ／パスコードで符号化できるメッセージ内容128を含み、このパスフレーズは、所与の電光サインシステム内の装置のメーカー（Sony社など）に一意のものとする事ができ、或いはサインネットワーク管理者などが決定するようなシステム自体に一意のものとする事ができると理解される。これに関わらず、図7には、メッセージテイル116が上述のシークレットコードを含むことができることも示している。

【0055】

詳細な説明を続けると、上述したように、1又はそれ以上のノードは、他のノードを発見してこれに接続することができる（例えば、電光サインは、最初の通電時に制御サーバを発見してこれに接続する）。例示的な実施形態では、電光サインなどによって行われる発見及び対応する接続を、発見要求メッセージなどのメッセージがセキュアな状態を保って悪意ある攻撃の影響を受けないようにセキュアに実行することができる。上記に従い、発見処理のための例示的なタイムアウト及びリトライ値を以下に示す。

例えば、（場合によってはインターネットを介して）Sony社の専用サーバを発見した場合、

```
#define TIMEOUT_DISC_REQ 1000000 /* 10 second * /  
#define RETRY_NET_SCAN 20
```

例えば、（場合によってはローカルネットワーク上で）ローカル制御サーバを発見した場合、

```
#define TIMEOUT_DISC_REQ 1000000 /* 1 second * /  
#define RETRY_NET_SCAN 3
```

【0056】

特に発見要求メッセージに関しては、顧客現場において通電された電光サインなどの専用装置（以下で一例として参照するようなSony社のシステム内のSony社のTVなど）からメッセージを送信することができ、このメッセージは、Sony社のインターネットサーバ、又はやはりSony社のサーバとすることができるローカル制御サーバを発見して接続しようとする試みにおいて送出される。この場合も、このメッセージは、Sony社のネットワーク専用とすることができ、従って、Sony社のインターネットサーバ又はローカルコントローラサーバ上で実行中のSony社のソフトウェアによってのみ確認応答される。

【0057】

さらに、Sony社以外の装置又は未承認の装置などからのサービス妨害（DOS）攻撃からネットワークを保護するために、発見要求メッセージは、64ビットなどを含むセキュリティフィールドを含むことができる。8バイトは、本明細書で説明するSony社の秘密アルゴリズムから導出される。従って、アルゴリズムへの入力は、Sony社の秘密鍵及び新たなノードが接続しようとするネットワークのESSIDとすることができる。受信側（Sony社のサーバなどの発見要求メッセージを受け取るノードなど）では、予想した結果にセキュリティフィールドが一致しない場合、それ以上発見要求メッセージが処理されず、受信側ノードは発見応答メッセージを送信しない。

【0058】

以下の表に、発見要求メッセージ処理中に使用できる及び／又は発見要求メッセージに含めることができる例示的な情報を示す。

パケット内容	サイズ (バイト単位)	ビットフォーマット (任意)
ソフトウェアバージョン	1	0 0 0 0 0 0 0 1
トランザクションID	2	—
サーバ発見	1	0 1 0 1 0 0 0 0
チャレンジテキスト	8	—
繰り返されるコード (0 x 5 A) のコード長	4	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0

10

0 0 0 0 0 0 0 1	—	0 0 0 1 0 0 0 1	—	—	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
--------------------	---	--------------------	---	---	---

【0059】

なお、送信側ノード（電光サインなど）は、発見要求メッセージを送信した後、Sony社のサーバなどが発見要求メッセージを処理した後に、このSony社のサーバから発見応答メッセージを受け取ることができる。発見応答メッセージは、（Sony社などの）セキュリティ鍵、及び要求側ノードが電光サインネットワークに接続するために必要とし得るその他のパラメータを含むことができる。発見応答メッセージは、サーバ（ローカルコントローラ又はSony社の遠隔サーバなど）の公開鍵をさらに含むことができる。さらに、さらなる保護のために、公開鍵のチェックサムを提供することができる。

20

【0060】

また、例示的な実施形態では、これらの鍵（公開鍵／秘密鍵のペア）を、opensslを使用して生成することができ、公開鍵のチェックサムを、md5sumを使用して生成することができる。また、発見応答メッセージは、中間者（MITM）攻撃から保護するために、64ビットを含むセキュリティフィールドを含むことができる。8バイトは、Sony社の秘密アルゴリズムから導出される。アルゴリズムへの入力は、（上述したものと同一のものなどの）Sony社の秘密鍵及び発見応答メッセージを送信するノード（Sony社のサーバなど）のMACアドレスとすることができる。受信側ノード（Sony社の電光サインなど）は、発見応答メッセージを受け取ると、対応する動作を実行し、セキュリティフィールド内のビットが一致しない場合には、発見応答メッセージを無視する。従って、このスキームは、正規のSony社の接続を乗っ取る偽のノードからの保護を行うものであると理解することができる。

30

【0061】

以下の表に、発見応答メッセージ処理中に使用できる及び／又は発見応答メッセージに含めることができる例示的な情報を示す。

パケット内容	サイズ (バイト単位)	ビットフォーマット (任意)
ソフトウェアバージョン	1	0 0 0 0 0 0 0 1
トランザクションID	2	—
サーバ応答	1	0 1 1 1 0 0 0 0
公開鍵	2 7 2	—
チェックサム	3 3	—
チャレンジテキスト	8	—
繰り返されるコード (0 x 5 A) のコード長	4	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0

10

0 0 0		0 0 0	—	—	—	0 1 0 1 1 0 1 0 0 1
0 0 0		1 0 0				0 1 1 0 1 0 0 1 0 1
0 1		0 1				1 0 1 0 0 1 0 1 1 0
						1 0

【0 0 6 2】

20

次に、本原理は、上述したような発見応答メッセージをノード（発見要求メッセージを送信した電光サインなど）において受け取ると、この発見応答メッセージを受け取ったノードは、受け取ったチェックサムを、受け取った公開鍵のローカルに生成されたチェックサムと比較することにより、メッセージの完全性をチェックすることも認識する。発見応答メッセージを受け取ったノードは、チェックサムが確認されると、発見応答メッセージを送信したノード（制御サーバなど）の公開鍵、MACアドレス及びその他の詳細を、ノード上のコンピュータ可読記憶媒体に記憶することができる。

【0 0 6 3】

本原理は、発見要求及び応答メッセージが上述したように処理された後に「認証フェーズ」が行われることをさらに認識する。このような認証フェーズでは、ネットワーク「パスフレーズ」を以下に示すように使用することができる。パスフレーズは、ノードのセキュアなメモリに埋め込むことなどもでき（及びSony社などの装置メーカーに対して一意、及び／又は各顧客、ネットワーク環境及び／又は広告現場に対して一意とすることもでき）、或いはネットワーク管理者がネットワーク／サブネット内の各ノード／装置にパスフレーズを提供することもできる。

30

【0 0 6 4】

本原理は、本明細書で説明するネットワーク／サブネット内のノードが、それぞれのセキュアなメモリに埋め込まれたパスフレーズを有することができる少なくとも1つの理由がある場合には、いくつかの機能を自動化すること、及び／又は新たなノードをサブネットに容易に接続することが望ましいことも認識する。従って、電光サインなどのノードが、認証フェーズ中にメッセージ（以下で簡単に説明する接続要求メッセージなど）を送信する場合、制御サーバの公開鍵を用いてパスフレーズを暗号化し、チェックサムパラメータ及び送信側ノードの公開鍵と共に送信することができる。その後、受信側ノードは、その記憶したパスフレーズと復号したパスフレーズを比較することができる。これら2つが一致する場合、サーバは、サーバにメッセージを送信したノードに、成功応答通知をメッセージ（やはり以下で簡単に説明する接続確認メッセージなど）に含めて返送することができる。

40

【0 0 6 5】

認証フェーズに関して上述した内容によれば、接続認証処理のためのタイムアウト及びリトライ値を以下の通りとすることができる。

50

例えば、（インターネットを介して）Sony社の制御サーバを発見した場合、

```
#define TIMEOUT_CONN_REQ 15 /* 15 seconds
* /
```

```
#define MAX_CONN_RETRY 20
```

例えば、（サブネットなどのローカルネットワークなどを介して通信し）「ローカル」制御サーバを発見した場合、

```
#define TIMEOUT_CONN_REQ 5 /* 5 seconds
* /
```

```
#define MAX_CONN_RETRY 3
```

【0066】

上述したように、本原理による「認証フェーズ」中に制御サーバにアクセスする場合には、電光サインなどのノードが接続確認メッセージを送信することができる。サブネットに参加するノードは、上述した発見要求及び応答メッセージの交換などを含む「発見フェーズ」後に繰り返すために、その後、セキュアな方法で制御サーバに接続するように試みることができる。やはり上述したように、参加ノードは、受け取った発見応答メッセージに基づいて、サーバのMACアドレス、公開鍵及びその他のパラメータを記憶することができる。次に、参加ノードは、上述したようなパスフレーズ、参加ノードの公開鍵及び両方のチェックサムを含む接続要求メッセージを送信することができる。接続要求メッセージは、エラーコード及びリトライカウンタを含むこともできる。この情報を接続確認メッセージと共に使用して、参加ノードと制御サーバの間に接続エラーが生じた場合に適切に動作することができる。

【0067】

以下の表に、接続要求メッセージ処理中に使用可能な、及び／又は接続要求メッセージに含めることができる例示的な情報を示す。

パケット内容	サイズ (バイト単位)	ビットフォーマット (任意)
ソフトウェアバージョン	1	00000001
トランザクションID	2	—
サーバ要求	1	10000000
リトライ	1	—
エラーコード	1	—
暗号化されたパスフレーズ	128	—
暗号化されたパスフレーズの ためのチェックサム	33	—
公開鍵	272	—
公開鍵のためのチェックサム	33	—
チャレンジテキスト	32	—
繰り返されるコード(0x5A) のコード長	4	010110100101 101001011010 01011010

0000	—	000	—	—	—	—	—	—	—	01011010010110
0001		100								10010110100101
		11								1010

【0068】

この認証フェーズについての説明を続けると、制御サーバが、上述したような接続要求

メッセージを受け取った後、電光サインなどのノードがネットワーク／サブネットに参加するための処理における別の任意の最終ステップは、応答コードを含む確認（接続確認メッセージなど）を制御サーバが参加ノードに送信することである。この応答コードは、参加ノードの接続要求を制御サーバが受け取ったこと、及び認証された接続への試みが成功又は失敗のいずれかであったことを示す、参加ノードへのフィードバックとしての役割を果たすことができる。従って、制御サーバは、接続要求メッセージを受け取ると、チェックサム値を調べることによって完全性をチェックする。次に、制御サーバは、暗号化されたパスフレーズを復号して、受け取った公開鍵の完全性をチェックすることができる。

【0069】

以下は、上述した原理による、例示的な成功及びエラーコードの非排他的なリストである。

```
#define CONN_SUCCESS
#define PASSCODE_FAILED 1
#define ENC_CHKSUM_ERR 2
#define PUBKEY_CHKSUM_ERR 3
#define UNKNOWN_ERR 4
```

【0070】

さらに、接続確認メッセージは、中間者（MITM）攻撃から保護するために、64ビットなどを含むセキュリティフィールドを含むことができる。8バイトは、Sony社の秘密アルゴリズムなどから導出される。従って、アルゴリズムへの入力、Sony社の秘密鍵及び制御サーバのMACアドレスとすることができる。受信側ノード（参加ノードなど）は、同様の動作を実行し、セキュリティフィールド内のビットが一致しない場合には、参加装置は接続確認メッセージを無視する。従って、上述したメッセージ及び処理は、偽の装置及び／又は不当な攻撃が正規のネットワーク及び／又はサブネット接続を乗っ取るのを防ぐことができる。

【0071】

以下の表に、接続確認メッセージ処理中に使用可能な、及び／又は接続確認メッセージに含めることができる例示的な情報を示す。

パケット内容	サイズ (バイト単位)	ビットフォーマット (任意)
ソフトウェアバージョン	1	00000001
トランザクションID	2	—
サーバ確認	1	10010000
応答コード	1	—
チャレンジテキスト	8	—
繰り返されるコード10x 5A} のコード長	4	010110100101 101001011010 01011010

000 000 01	—	0001 0100	—	—	010110100101101001011 01001011010
------------------	---	--------------	---	---	--------------------------------------

【0072】

上述した発見及び認証フェーズの処理を示すために、図8及び図9に注目されたい。図8には、参加ノードが制御サーバを発見できない場合を示しており、図9には、制御サーバをうまく発見して認証処理を行う場合を示している。

【0073】

まず図8から説明すると、この図には、電光サインなどの参加ノードが、制御サーバを発見するための発見要求メッセージを、例えばサブネット上でローカルに及び／又はインターネットを介して送信することを表す第1の矢印150を示している。図8には、発見要求メッセージを受け取ったサーバから何らかの理由で送信されない、及び／又は別の理由で参加ノードが受け取らなかったと予想される発見応答メッセージを示す破線矢印152も示している。

【0074】

次に、参加ノードは、矢印154で示すような第2の発見要求メッセージを送信することができる。この場合も、予想される発見応答メッセージがサーバから送信されず、及び／又は別の理由で参加ノードが受け取らなかったことを示す別の破線矢印156を示している。図6と同様に、図8に示すように、 t は、送信側から1「ホップ」だけ離れたノードにメッセージが届くのに要する最大時間を定義し、「 p 」は、サーバなどの受信側ノードがメッセージを処理するのに必要な時間の上限を定義し、この結果、参加ノードが発見応答メッセージなどを受け取るための最大時間は $(2t + p)$ となる。また、図8には、破線矢印158によって示すように、参加ノードが少なくとも1つの発見応答メッセージを受け取れなかった後、タイムアウトが発生するまでに発見要求メッセージを少なくとも r 回送出することも示している。

【0075】

図9には、本原理による正常な発見及び認証フェーズの説明図を示している。矢印160は、参加ノードから発見要求メッセージが送信され、制御サーバがこれを受け取ることを示しており、矢印162は、次に制御サーバにより発見応答メッセージが送信され、参加ノードがこれを受け取ることを示している。また、矢印164は、その後、発見要求メッセージに応答した制御サーバに接続要求メッセージが送信され、このサーバがこれを受け取ることを示しており、矢印166は、次にサーバが接続確認メッセージを送信し、参加ノードがこれを受け取ることを示している。

【0076】

この詳細な説明を続けると、いくつかの実施形態では、本原理によるネットワーク及び／又はサブネットに参加したノードが制御サーバから接続したいと思う場合がある。例えば、電光サインのサブネットを運営する電光サインの顧客が、接続された制御サーバから装置を接続する能力を持ちたいと望むことがある。従って、（電光サインなどの）ノードは、本明細書で説明するメッセージ交換原理に従い、制御サーバにサーバ接続メッセージを送信することができる。例えば、このサーバ接続メッセージは、Sony社の電光サインサブネットをハッキングするSony社以外の装置などから送出された偽の及び／又は乗っ取られたサーバ接続メッセージからネットワーク／サブネットを保護するために、64ビットなどのセキュリティフィールドを含むことができる。8バイトは、本原理による秘密アルゴリズムから導出することができる。さらに、アルゴリズムへの入力、Sony社の秘密鍵、及びサーバ接続メッセージを送信するノードのMACアドレスとすることができる。従って、いくつかの実施形態では、サーバ接続メッセージが、シークレットコード（サブネット固有のセキュリティフィールドなど）を含むことができる。

【0077】

以下の表に、サーバ接続処理中に使用可能な、及び／又はサーバ接続メッセージに含めることができる例示的な情報を示す。

パケット内容	サイズ (バイト単位)	ビットフォーマット (任意)
ソフトウェアバージョン	1	0 0 0 0 0 0 0 1
サーバ発見	1	1 0 1 0 0 0 0 0
チャレンジテキスト	8	—
繰り返されるコード (NSA)) のコード長	4	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0

0 0 0 0 0 0 0 1	—	0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
-----------------	---	---

【0078】

図10に、本原理による正常な発見及び認証フェーズの別の説明図を示す。矢印170は、参加ノードから発見要求メッセージが送信され、制御サーバがこれを受け取ることを示しており、矢印172は、次に制御サーバにより発見応答メッセージが送信され、参加ノードがこれを受け取ることを示している。また、矢印174は、その後、発見要求メッセージに回答した制御サーバに接続要求メッセージが送信され、このサーバがこれを受け取ることを示しており、矢印176は、次にサーバが接続確認メッセージを送信し、参加ノードがこれを受け取ることを示している。

【0079】

比較すると、図10は、送信されるメッセージごとに矢印の近くにメッセージ情報も示しているという点で図9よりも詳細である。従って、発見メッセージは、MSG__DISC__REQ及びMSG__DISC__RSPであり、接続認証メッセージは、MSG__CONN__REQ及びMSG__CONN__CFMである。これらのメッセージは、本明細書で説明する原理による、Sony社の一意の装置ID及びSony社固有のアルゴリズムによって計算された特殊なビットフォーマットなどを含む図示のチャレンジテキストフィールドによって保護することができると理解されたい。

【0080】

次に図11を参照すると、本原理による、ネットワーク/サブネットに参加するノードにより実行されるロジック例のフローチャートを示している。ブロック180から開始して、参加ノードが発見要求メッセージを送信し、サーバからの発見応答メッセージを待つ。次に、ロジックは、菱形判定ブロック182において、発見応答メッセージが受け取られたかどうか、及び/又は発見要求メッセージの送信をリトライすべきか、それともタイムアウトすべきかを判断する。参加ノードが発見要求メッセージを再送すべきであると判断した場合、ロジックはブロック180に戻る。なお、タイムアウトすべきであると判断した場合、ロジックは菱形判定ブロック182で中止することができる。

【0081】

一方、菱形判定ブロック182において、制御サーバなどから発見応答メッセージが送信されていると判断された場合、ロジックはブロック184に進んで発見応答メッセージを受け取る。次に、ロジックはブロック186に進んでチェックサムを確認し、制御サーバから受け取った、参加ノードが参加しようとしているネットワーク/サブネット内のノードの公開鍵及びチェックサムを記憶する。その後、ロジックはブロック188に進み、必要に応じてユーザ/ネットワーク管理者に上述したようなパスフレーズを促すことができ、及び/又は参加ノードのセキュアなメモリからパスフレーズを読み出すことができる。ロジックは、パスフレーズがロジックによりどのように受け取られ及び/又は読み出されるかに関わらず、ブロック190において、パスフレーズを制御サーバの公開鍵で暗号化する。ロジックは、ブロック190において、参加ノードの公開鍵及び対応するチェッ

10

20

30

40

50

クサムを含むことができる、暗号化したフレーズ及びこのチェックサムを含む接続要求メッセージも送信する。

【0082】

次に、ブロック192において、ロジックは、菱形判定ブロック194に進む前に接続確認メッセージを待つ。菱形判定ブロック194において、ロジックは、タイムアウトすべきか、及び／又は接続要求メッセージを再送すべきかどうかを判断する。ロジックは、タイムアウトすべきであると判断した場合、終了するか又はブロック188に戻ることができる。一方、接続要求メッセージを再送すべきであると判断した場合、菱形判定ブロック196に示すように、接続確認メッセージが受け取られたと判断されるまで再送を行う。また、図10に示すように、ロジックは、接続確認メッセージは受け取ったものの、参加ノードが求める接続に失敗したことをメッセージが示していると判断した場合、ブロック188に戻り及び／又は終了することができる。一方、接続確認メッセージが、正常に接続が行われたことを示している場合、ロジックはブロック198に進み、認証処理がうまくいき、参加ノードが正常に制御サーバに接続したことを認識する。

10

【0083】

図12に、詳細な説明のまとめとして、電光サインなどのノードがネットワーク／サブネットに参加しようとする場合に制御サーバにより実行される例示的なフローチャートを示している。ロジックは、円形ブロック250から開始してブロック252に進み、制御サーバのロジックが、サーバのバックグラウンド処理などを使用して発見要求メッセージが受け取られるのを待つ。

20

【0084】

ロジックは、ブロック252において発見要求メッセージを受け取った後、次に菱形判定ブロック254に進み、受け取った暗号化されたメッセージのチェックサムを確認する。メッセージがエラーを含む場合、ロジックはブロック256に進み、パズフレーズチェックサムエラー通知を含むメッセージを参加ノードに返送してブロック252に戻る。一方、メッセージが、菱形判定ブロック254において判定されるようなエラーを含まない場合、ロジックはブロック252ではなく菱形判定ブロック258に進み、受け取った公開鍵のチェックサムを確認する。ロジックは、受け取ったメッセージがこの点でエラーを含むかどうかを判定し、含む場合にはブロック260に進み、公開鍵チェックサムエラー通知を含むメッセージを参加ノードに返送してブロック252に戻る。一方、メッセージが、菱形判定ブロック258で判定されるようなエラーを含まない場合、ロジックは、ブロック260ではなく菱形判定ブロック262に進む。

30

【0085】

ロジックは、菱形判定ブロック262において、復号されたパズフレーズが、ローカルに記憶された（例えば、本原理による、制御サーバのコンピュータ可読記憶媒体に記憶及び／又はプログラムされた）パズフレーズに一致するかどうかを判定する。パズフレーズが一致しないと判定した場合、ロジックはブロック264に進み、パズフレーズエラー通知を含むメッセージを参加ノードに返送してブロック252に戻る。一方、パズフレーズが一致する場合、ロジックはブロック264ではなくブロック266に進み、（例えば、装置の記憶媒体上の）装置リストテーブル内に新たなノードのエントリを作成し、参加ノードが求める接続に成功したことを示す接続確認メッセージを参加ノードに送信する。

40

【0086】

従って、本原理は、電光サインが電光サインのネットワーク及びサブネットにセキュアに、容易に、かつ自動的に参加するためのシステム及び方法を提供するものであると理解することができる。完全性を期すために、たとえ上記のいずれの部分にも具体的に記載していなくても、上述したメッセージ（発見要求又は応答メッセージなど）には、上述したメッセージ情報の全部又は一部を適宜使用することができる。例えば、公開鍵及びサブネットアドレスは、（発見又は認証などの）いずれかの「フェーズ」中の望ましい時に交換及び／又は送信することができる。

【0087】

50

さらに、上述のメッセージは、電光サインを動作するように及び／又は特定の広告又は一連の広告を表示するように構成するための他の構成コマンドを含むこともでき、必要に応じてIPネットワーク設定を含むこともできる。最後に、制御サーバと電光サインの間のノード（ルータなど）は、意図する受信側（サーバ又は電光サインなど）にメッセージが届くように、上述したメッセージを全て転送できると理解されたい。また、（新たなルータがサブネットに参加する場合などの）サブネット環境によっては、ルータが、必要に応じてルータ自体の発見、構成及び／又は認証メッセージを生成することもできる。

【 0 0 8 8 】

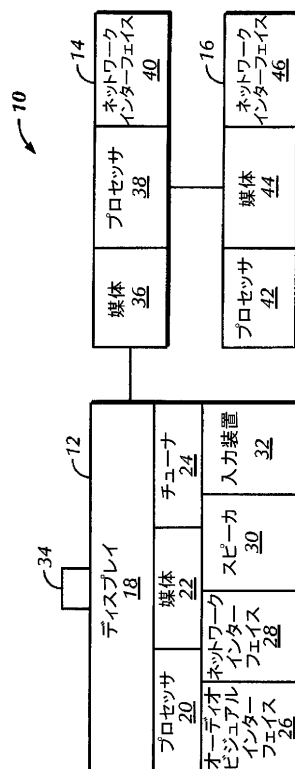
上述した図及び説明は、一般に本明細書で開示した装置と連動する方法ステップを示しているとして理解されたい。

【 0 0 8 9 】

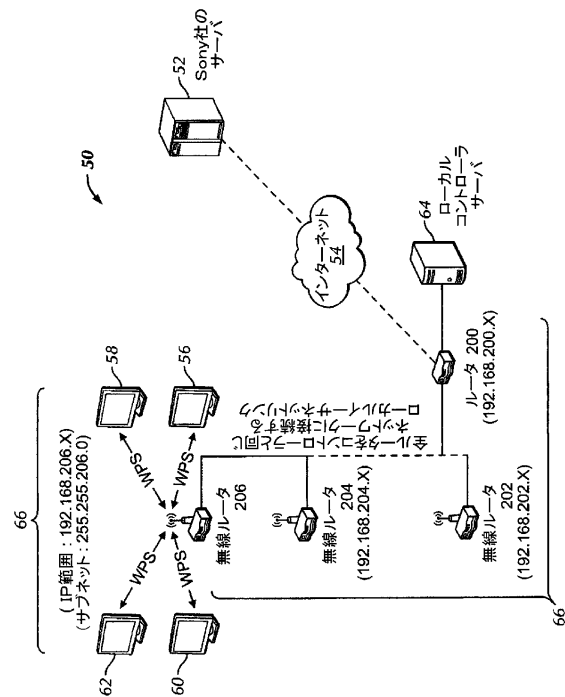
本明細書では、広告現場において電光サインを動作するように構成するためのシステム及び方法について詳細に図示し説明したが、本発明が含む主題は、特許請求の範囲によってのみ限定されるものであると理解されたい。

10

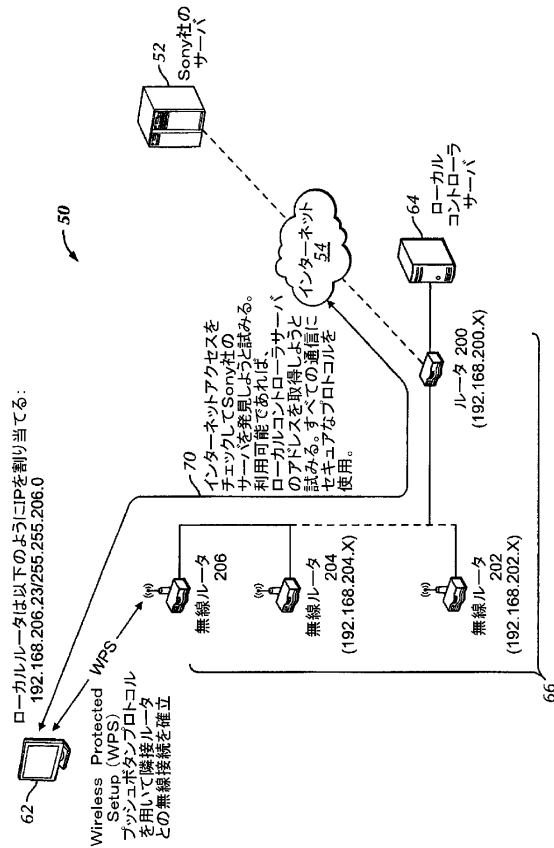
【図 1】



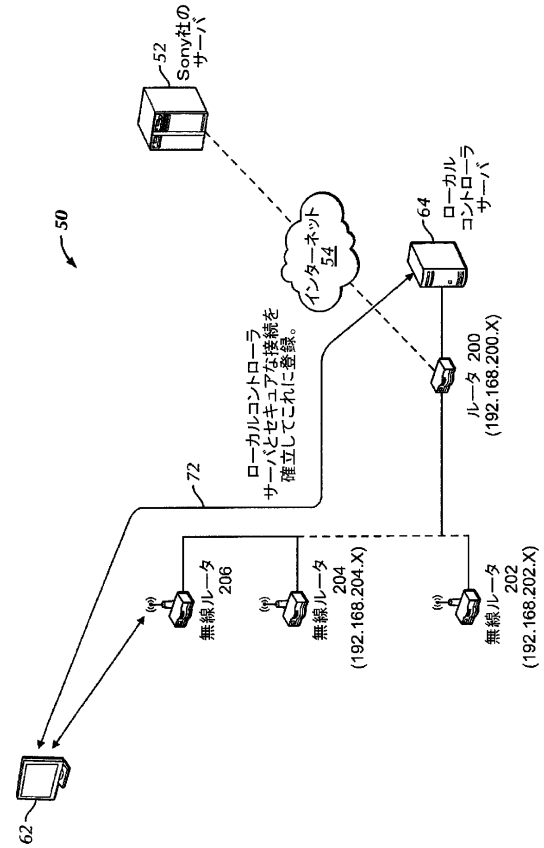
【図 2】



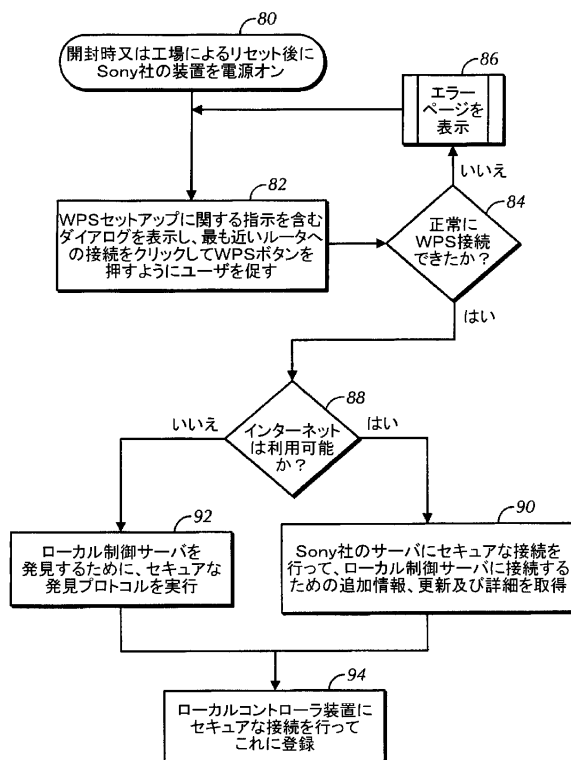
【図 3】



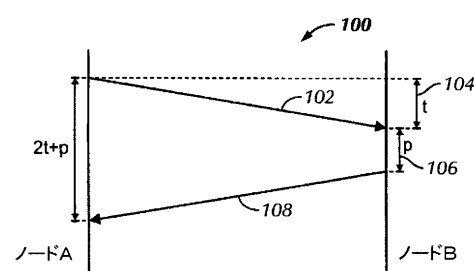
【図 4】



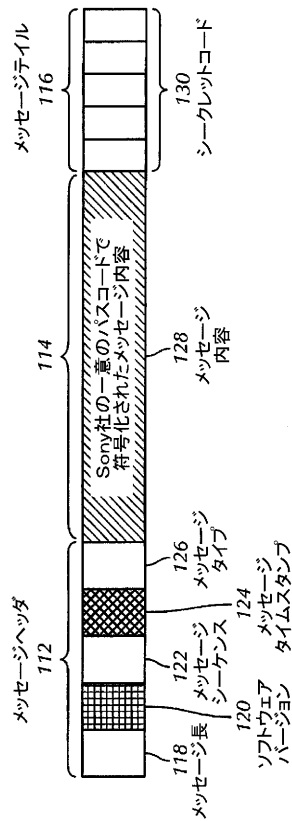
【図 5】



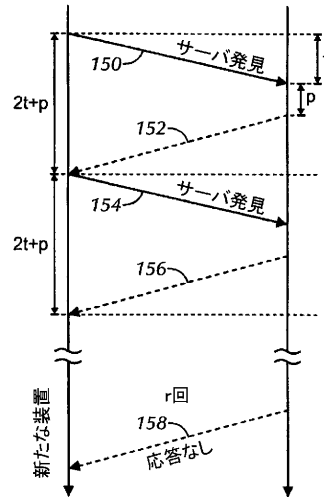
【図 6】



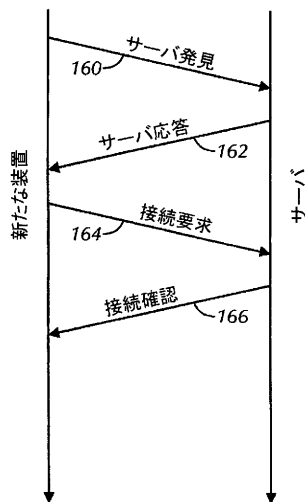
【図 7】



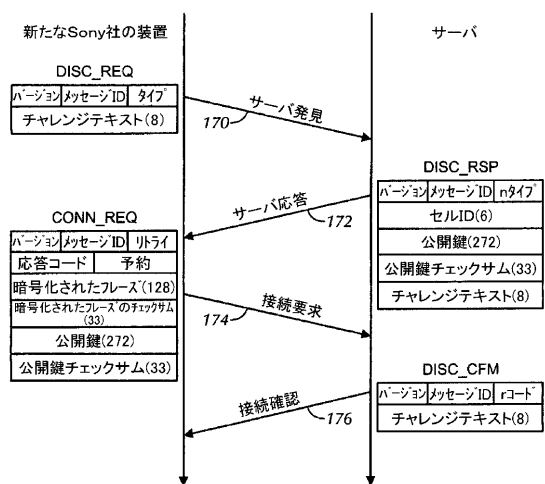
【図 8】



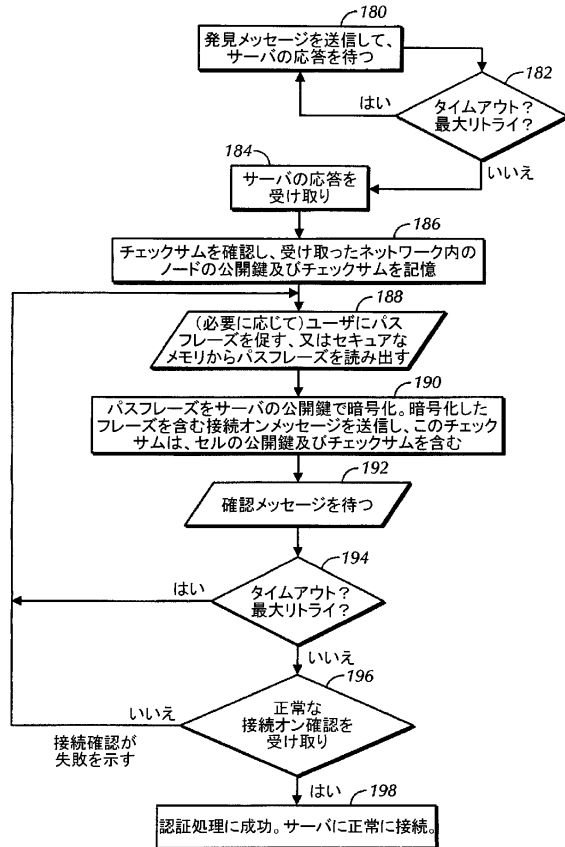
【図 9】



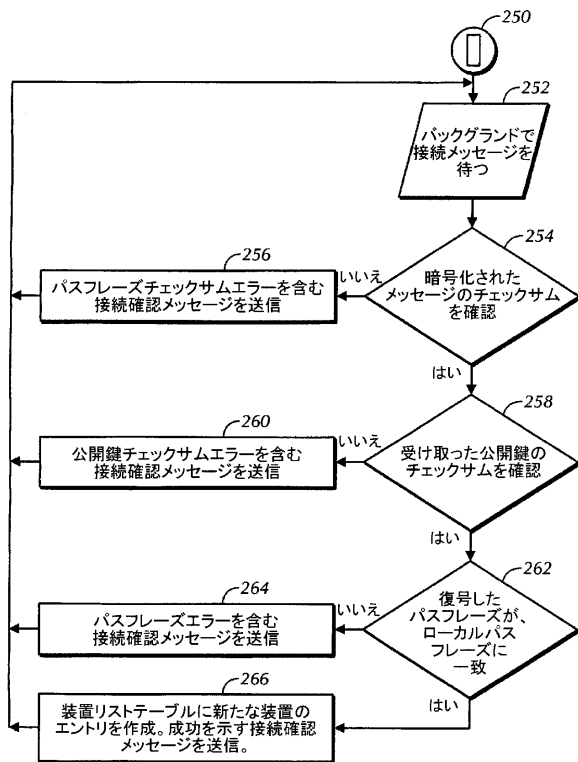
【図 10】



【図 11】



【図 12】



フロントページの続き

- (72)発明者 アビシェーク ピー パティル
アメリカ合衆国 カリフォルニア州 92127 サン ディエゴ リザーヴ ドライヴ 103
35 #103
- (72)発明者 タンメイ アグニホートリ
アメリカ合衆国 カリフォルニア州 92128 サン ディエゴ アルタ カーメル コート
12023 #259
- (72)発明者 金 東郁
アメリカ合衆国 カリフォルニア州 92127 サン ディエゴ アヴェニダ デ ロス ロボ
ス 11333 アpartment シー

審査官 安藤 一道

- (56)参考文献 特開2012-076681 (JP, A)
特開2012-060476 (JP, A)
特開2012-060475 (JP, A)
特開2004-120462 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| H04L | 12/46 |
| H04L | 12/66 |
| H04W | 12/08 |
| H04W | 76/02 |
| H04W | 84/12 |