

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6959155号
(P6959155)

(45) 発行日 令和3年11月2日(2021.11.2)

(24) 登録日 令和3年10月11日(2021.10.11)

(51) Int.Cl.	F I
H04L 9/32 (2006.01)	H04L 9/00 675B
G06F 21/64 (2013.01)	G06F 21/64

請求項の数 10 (全 25 頁)

(21) 出願番号	特願2018-9147 (P2018-9147)	(73) 特許権者	514136668
(22) 出願日	平成30年1月23日 (2018.1.23)		パナソニック インテレクチュアル プロ
(65) 公開番号	特開2018-196108 (P2018-196108A)		パティ コーポレーション オブ アメリ
(43) 公開日	平成30年12月6日 (2018.12.6)		カ
審査請求日	令和2年9月15日 (2020.9.15)		Panasonic Intellectual
(31) 優先権主張番号	特願2017-96225 (P2017-96225)		Property Corporation of America
(32) 優先日	平成29年5月15日 (2017.5.15)		アメリカ合衆国 90504 カリフォル
(33) 優先権主張国・地域又は機関	日本国 (JP)		ニア州, トーランス, スイート 450,
			ウエスト 190ストリート 2050
		(74) 代理人	100109210
			弁理士 新居 広守
		(74) 代理人	100137235
			弁理士 寺谷 英作

最終頁に続く

(54) 【発明の名称】 検証方法、検証装置およびプログラム

(57) 【特許請求の範囲】

【請求項 1】

車両で利用されるコンテンツデータを検証する検証方法であって、
前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、

前記車両の状態を示す状態情報を取得し、

取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、

(a) 取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、(b) 生成した前記第二ハッシュ値と、(c) 取得した前記署名と、を用いて、前記コンテンツデータの検証を行い、

前記検証の結果を示す情報を出力する

検証方法。

【請求項 2】

前記第二ハッシュ値を生成する際には、前記複数の部分データから前記N個の部分データをランダムに選択し、選択した前記N個の部分データのそれぞれから第二ハッシュ値を生成する

請求項 1 に記載の検証方法。

10

20

【請求項 3】

前記状態情報は、前記車両が走行中であるか否かを示し、
前記第二ハッシュ値を生成する際には、
前記車両が走行中である場合には、前記Nを第1の値に定め、
前記車両が走行中でない場合には、前記Nを前記第1の値より大きい第2の値に定め、
定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成する

請求項1又は2に記載の検証方法。

【請求項 4】

前記状態情報は、前記車両の状態として、前記検証方法を実行する装置の処理負荷を示し、

前記第二ハッシュ値を生成する際には、

前記処理負荷が高いほど、前記Nをより小さな値に定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成する

請求項1～3のいずれか1項に記載の検証方法。

【請求項 5】

前記状態情報は、前記車両の状態として、前記検証方法を実行する装置が行う通信の通信量を示し、

前記第二ハッシュ値を生成する際には、

前記通信量が多いほど、前記Nをより小さな値に定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成する

請求項1～4のいずれか1項に記載の検証方法。

【請求項 6】

前記第二ハッシュ値を生成する際には、前記コンテンツデータの種類またはサイズに応じて前記Nを定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成する

請求項1～5のいずれか1項に記載の検証方法。

【請求項 7】

前記第二ハッシュ値を生成する際には、前記コンテンツデータの種類に基づいて、前記複数の部分データのうちのどの部分データを前記N個の部分データとして選択するかを決定し、当該決定に基づいて選択した前記N個の部分データのそれぞれから前記第二ハッシュ値を生成する

請求項1～6のいずれか1項に記載の検証方法。

【請求項 8】

前記コンテンツデータの種類は、前記コンテンツデータの更新の間隔を示す指標を含む
請求項6又は7に記載の検証方法。

【請求項 9】

車両で利用されるコンテンツデータを検証する検証装置であって、

プロセッサと、前記プロセッサに接続されたメモリとを備え、

前記プロセッサは、前記メモリを用いて、

前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、

前記車両の状態を示す状態情報を取得し、

取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、

(a) 取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、(b) 生成した前記第二ハッシュ値と、(c) 前記署名と、を用いて、前記コンテンツデータの検証を行い、

10

20

30

40

50

前記検証の結果を示す情報を出力する
検証装置。

【請求項 10】

請求項 1～8 のいずれか 1 項に記載された検証方法を、プロセッサに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、コンテンツデータを検証する検証方法、検証装置およびプログラムに関する 10

【背景技術】

【0002】

近年、車両の自動運転車を制御する自動運転システムが知られている。自動運転システムでは、制御の基盤となる高度な地図データ、並びに、自動車、歩行者及びインフラ設備などの情報は、車外の装置との通信により入手することが想定されている。例えば、車車間通信又は路車間通信などの V2X (Vehicle to Everything) による通信で情報を入手したり、情報端末との通信で情報を入手したり、様々な通信で情報の入手を行う。そして、これらの入手した情報、車両の走行状態、車両の周辺状況及び運転者の状態などを鑑みて、自動運転車の制御が行われる。 20

【0003】

特許文献 1 では、車両の自動運転制御の安全性を高めるために、自動運転車両制御装置が自動運転を行うための条件を満たしていないと判断した場合には、運転者に対して自動運転の解除を促す通知を行う構成が開示されている。

【先行技術文献】

【特許文献】

【0004】

【特許文献 1】特開 2014-106854 号公報

【非特許文献】

【0005】

【非特許文献 1】「Federal Information Processing Standards Publication 186-4 DIGITAL SIGNATURE STANDARD (DSS)」、2013年7月、National Institute of Standards and Technology (NIST)

【発明の概要】

【発明が解決しようとする課題】

【0006】

自動運転システムが車外の装置からデータを入手する場合、不正な端末が成りすましによって不正なデータを送信するなどのサイバー攻撃が懸念される。

【0007】

一方、従来のコンテンツデータの検証において、ダウンロードした地図データなどのコンテンツデータが大容量であると、コンテンツデータをすべて検証するには多大な時間を要する。そのため、ダウンロードしたコンテンツデータなどをすべて検証してから利用することを想定する場合、コンテンツデータをリアルタイムに車両の自動運転に利用できない、という問題がある。 40

【0008】

そこで、本発明は、車両の自動運転への利用に、より適したコンテンツの検証方法等を提供する。

【課題を解決するための手段】

【0009】

本発明の一態様に係る検証方法は、車両で利用されるコンテンツデータを検証する検証 50

方法であって、前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、前記車両の状態を示す状態情報を取得し、取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、(a)取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、(b)生成した前記第二ハッシュ値と、(c)取得した前記署名と、を用いて、前記コンテンツデータの検証を行い、前記検証の結果を示す情報を出力する検証方法である。

【0010】

なお、これらの包括的または具体的な態様は、システム、装置、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なCD-ROMなどの記録媒体で実現されてもよく、システム、装置、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。

【発明の効果】

【0011】

本発明によれば、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【図面の簡単な説明】

【0012】

【図1】図1は、実施の形態におけるコンテンツ検証システムの全体構成を示す模式図である。

【図2】図2は、実施の形態における車両の機能構成を示す模式図である。

【図3】図3は、実施の形態におけるゲートウェイの機能構成を示す模式図である。

【図4】図4は、実施の形態におけるサーバの機能構成を示す模式図である。

【図5】図5は、実施の形態における信号機の機能構成を示す模式図である。

【図6】図6は、実施の形態におけるサーバから車両へコンテンツデータをダウンロードする処理を示すシーケンス図である。

【図7】図7は、実施の形態におけるサーバによるコンテンツデータを生成する処理を示すフローチャートである。

【図8】図8は、実施の形態における検証可能なコンテンツデータを生成する処理の説明図である。

【図9】図9は、実施の形態における車両によるコンテンツデータを検証する処理を示すフローチャートである。

【図10】図10は、実施の形態におけるコンテンツデータを検証する処理の説明図である。

【図11】図11は、実施の形態における車両からサーバへセンサ情報をアップロードする処理を示すシーケンス図である。

【図12】図12は、実施の形態における信号機からサーバへセンサ情報をアップロードする処理を示すシーケンス図である。

【発明を実施するための形態】

【0013】

本発明の一態様に係る検証方法は、車両で利用されるコンテンツデータを検証する検証方法であって、前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、前記車両の状態を示す状態情報を取得し、取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、(a)取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、(b)生成した前記第二ハッシュ

値と、(c) 取得した前記署名と、を用いて、前記コンテンツデータの検証を行い、前記検証の結果を示す情報を出力する検証方法である。

【0014】

上記態様によれば、検証装置が、地図情報などを含む大容量のコンテンツデータを検証する場合に、コンテンツデータのうちの、車両の状態に応じて選択される一部を検証に用いるので、実用的なレベルで安全性を維持したまま、高速な検証が可能となり、安全なシステムの構築が可能となる。

【0015】

また、攻撃者は秘密鍵を持っておらず、攻撃者が正当な電子署名（単に署名ともいう）を生成することは困難であるので、検証装置は、コンテンツデータの検証用データに含まれる署名を用いて、コンテンツデータが正当であるか否かを検証でき、すなわち、攻撃者によるコンテンツデータの改ざんを検出できる。検証装置は、このようにコンテンツデータが正当であるか否かを検証できるので、その後に不正なコンテンツデータを破棄するなどして、車両の自動運転などの動作に正当なコンテンツデータのみを利用することによって、安全なシステムが構築できる。このように、検証装置は、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

10

【0016】

例えば、前記第二ハッシュ値を生成する際には、前記複数の部分データから前記N個の部分データをランダムに選択し、選択した前記N個の部分データのそれぞれから第二ハッシュ値を生成してもよい。

20

【0017】

上記態様によれば、検証装置は、地図情報などを含む大容量のコンテンツデータを検証する場合に、コンテンツデータの一部をランダムに選択して検証するので、実用的なレベルで安全性を維持したまま、高速な検証が可能となり、安全なシステムの構築が可能となる。

【0018】

ここで、車両におけるコンテンツデータの検証は、コンテンツデータを複数に分割した部分データのうち所定数をランダムに選択してなされる。そのため、システムへの攻撃者が、コンテンツデータを不正に改ざんした場合、選択した分割されたコンテンツデータの中に攻撃者による不正な改ざんが含まれる可能性が高い。よって、検証装置は、コンテンツデータが正当であるか否かをより適切に検証できるので、より安全なシステムが構築できる。

30

【0019】

言い換えれば、検証装置が、複数の部分データのうちのどの部分データを検証に使用するか毎回変化するので、成りすましなどによる悪意あるデータをより適切に検出することができる。よって、検証装置は、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【0020】

例えば、前記状態情報は、前記車両が走行中であるか否かを示し、前記第二ハッシュ値を生成する際には、前記車両が走行中である場合には、前記Nを第1の値に定め、前記車両が走行中でない場合には、前記Nを前記第1の値より大きい第2の値に定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成してもよい。

40

【0021】

上記態様によれば、検証装置は、検証のために確保できる時間が比較的長い場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる時間が比較的短い場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる時間の長短に応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

50

【0022】

例えば、前記状態情報は、前記車両の状態として、前記検証方法を実行する装置の処理負荷を示し、前記第二ハッシュ値を生成する際には、前記処理負荷が高いほど、前記Nをより小さな値に定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成してもよい。

【0023】

上記態様によれば、検証装置は、検証のために確保できる処理能力が比較的大きい場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる処理能力が比較的小さい場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる処理能力の大小

10

【0024】

例えば、前記状態情報は、前記車両の状態として、前記検証方法を実行する装置が行う通信の通信量を示し、前記第二ハッシュ値を生成する際には、前記通信量が多いほど、前記Nをより小さな値に定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成してもよい。

【0025】

上記態様によれば、検証装置は、通信量情報から得られる、検証のために確保できる処理能力が比較的大きい場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる処理能力が比較的小さい場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる処理能力の大小に応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

20

【0026】

例えば、前記第二ハッシュ値を生成する際には、前記コンテンツデータの種類またはサイズに応じて前記Nを定め、定めた前記Nを用いて、前記N個の部分データのそれぞれから前記第二ハッシュ値を生成してもよい。

【0027】

上記態様によれば、検証装置は、コンテンツデータの種類またはサイズに適した所定数の部分データを検証に用いることができる。よって、検証装置は、コンテンツデータの種類またはサイズに応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

30

【0028】

例えば、前記第二ハッシュ値を生成する際には、前記コンテンツデータの種類に基づいて、前記複数の部分データのうちのどの部分データを前記N個の部分データとして選択するかを決定し、当該決定に基づいて選択した前記N個の部分データのそれぞれから前記第二ハッシュ値を生成してもよい。

【0029】

上記態様によれば、検証装置は、コンテンツデータの種類に応じて、どの部分データにどのような内容のデータが含まれているかが既知である場合には、検証の必要性がより高い部分を検証の対象とすることができる。よって、検証装置は、検証の必要性がより高い部分を検証に用いることにより、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

40

【0030】

例えば、前記コンテンツデータの種類は、前記コンテンツデータの更新の間隔を示す指標を含んでもよい。

【0031】

上記態様によれば、検証装置は、コンテンツデータの更新の時間間隔を用いてコンテンツの種類を示し、車両の自動運転への利用に、より適したコンテンツの検証方法により、

50

コンテンツを検証できる。

【0032】

また、本発明の一態様に係る検証装置は、車両で利用されるコンテンツデータを検証する検証装置であって、プロセッサと、前記プロセッサに接続されたメモリとを備え、前記プロセッサは、前記メモリを用いて、前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、前記車両の状態を示す状態情報を取得し、取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、（a）取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、（b）生成した前記第二ハッシュ値と、（c）前記署名と、を用いて、前記コンテンツデータの検証を行い、前記検証の結果を示す情報を出力する。

10

【0033】

これによれば、上記検証装置と同様の効果を奏する。

【0034】

なお、これらの包括的または具体的な態様は、システム、装置、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なCD-ROMなどの記録媒体で実現されてもよく、システム、装置、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。

20

【0035】

以下、実施の形態について、図面を参照しながら具体的に説明する。

【0036】

なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

【0037】

（実施の形態）

30

1. システムの構成

本発明の実施の形態として、車載ネットワーク上に設置された検証装置であるゲートウェイが、車外の装置、より具体的には車外のサーバ又は信号機などからV2Xにより受信したコンテンツデータを検証する技術について図面を参照しながら説明する。

【0038】

1.1 コンテンツ検証システム10の全体構成

図1は、本実施の形態におけるコンテンツ検証システム10の全体構成を示す模式図である。図1において、コンテンツ検証システム10は、車両100a及び100bと、サーバ200と、信号機300とを備える。車両100a及び100bと、サーバ200と、信号機300とは、それぞれ通信可能に、ネットワーク又は通信リンクで接続されている。

40

【0039】

なお、コンテンツ検証システム10には、信号機300だけでなく、照明灯、情報掲示板標識、橋梁、トンネル及び横断歩道橋などのインフラ設備に取り付けられたセンサ、カメラ、並びに、GPS（Global Positioning System）受信器などがネットワーク又は通信リンクで接続されていてもよい。

【0040】

1.2 車両100aの構成

図2は、本実施の形態における車両100aの全体構成を示す模式図である。図2において、複数の電子制御ユニット（ECU：Electronic Control Un

50

it)であるECU111、ECU121、ECU131、ECU141、ECU151、ECU161、ECU171、ECU181及びECU191と、ゲートウェイ101とが、車載ネットワークで接続されている。車載ネットワークはController Area Network（以降、CAN）であってもよいし、Ethernet（登録商標）であってもよいし、CANとEthernet（登録商標）とが混在していてもよい。

【0041】

車載ネットワークには、例えば、エンジン110、トランスミッション120、モータ（不図示）、燃料（不図示）、又は、電池（不図示）の制御に関連する駆動系のECUが接続されている。本図では、車載ネットワークには駆動系のECUとして、エンジン110用のECU111と、トランスミッション120用のECU121とが接続されている。

10

【0042】

また、車載ネットワークには、ブレーキ130又はステアリング140などの、車両の「曲がる、止まる」機能に関連するシャーシ系ECUが接続されている。本図では、車載ネットワークにはシャーシ系ECUとして、ブレーキ130用のECU131と、ステアリング140用のECU141とが接続されている。

【0043】

また、車載ネットワークには、自動ブレーキ150、車線維持装置160、車間距離制御機能（不図示）、衝突防止機能又はエアバッグなどの安全快適機能系ECUが接続されている。本図では、車載ネットワークには安全快適機能系ECUとして、自動ブレーキ150用のECU151と、車線維持装置160用のECU161とが接続されている。

20

【0044】

また、車載ネットワークには、車車間通信装置170などに関連する通信系ECUが接続されている。本図では、車載ネットワークには通信系ECUとして、車車間通信装置170用のECU171が接続されている。車車間通信装置170は、他の車両からコンテンツデータを取得する。ECU171は、取得したコンテンツデータを用いて自動運転などの動作処理を行う。

【0045】

また、車載ネットワークには、ヘッドユニット180などインフォテイメント系ECUが接続されている。本図では、車載ネットワークにはインフォテイメント系ECUとして、ヘッドユニット180用のECU181が接続されている。なお、ヘッドユニット180用のECU181がなく、ヘッドユニット180がECU181を介さず直接車載ネットワークに接続されていてもよい。

30

【0046】

また、車載ネットワークには、高度道路交通システムであるITS（Intelligent Transport Systems）装置190用のECU191が接続されている。本図では、車載ネットワークには、ITS装置190用のECU191が接続されている。ITS装置190は、サーバ200が保有している路面情報及び地図情報などをサーバ200から受信する。また、ITS装置190は、センサ情報やGPSによる位置情報、カメラの画像情報などをサーバ200に送信する。ITS装置190から送信された画像情報によって、サーバ200は、道路状況などを把握することができる。

40

【0047】

また、図示しない各種センサ又はカメラの画像情報なども車載ネットワークには接続されている。

【0048】

ゲートウェイ101は、上記の各ECUに接続され、各ECUの間の通信を中継する中継装置である。上記の各ECUは、ゲートウェイ101を介して接続され、相互に情報をやりとりする。

【0049】

50

サーバ２００は、さまざまな種類のコンテンツデータを保有しており、各種情報処理を行うサーバ装置である。サーバ２００は、地図情報、路面情報、交通規制情報、事故情報、及び、歩行者情報などをコンテンツデータとして保有している。地図情報は、道路又は建物などの静的な地物を示す情報である。路面情報は、道路の路面の状態を示す情報である。交通規制情報は、天候又は事故などに起因した交通規制が行われている場所及び時間帯などを示す情報である。事故情報は、車両の事故が起こっている場所及び時刻などを示す情報である。歩行者情報は、歩行者がいる場所及び時刻などを示す情報である。サーバ２００は、車両１００aと通信回線を介して通信可能に接続されており、保有している各情報を車両１００aなどに提供する。

【００５０】

10

サーバ２００が保有しているコンテンツデータには、更新間隔が比較的長いものもあれば、比較的短いものもある。例えば、地図情報及び路面情報などは、数カ月程度の間隔で更新される。一方、事故情報及び交通規制情報などは、数時間から数分程度の間隔で更新される。サーバ２００は、各コンテンツデータに紐付けて、各コンテンツデータの更新間隔を示す指標を保有していてもよい。更新間隔を示す指標は、更新間隔の時間長（１カ月、１時間、１分又は１秒など）であってもよいし、更新間隔の程度を例えば３段階で示す指標（長い、中程度、短い）であってもよい。

【００５１】

信号機３００は、交通信号機である。信号機３００は、電波による通信、又は、可視光通信などによって、車両１００aなどと通信する。

20

【００５２】

１．３ ゲートウェイ１０１の構成

図３は、本実施の形態におけるゲートウェイ１０１の構成図である。図３においてゲートウェイ１０１は、コンテンツ検証部１００１、鍵保持部１００２、メッセージ処理部１００３、車両状態保持部１００４、及び、通信部１００５を含んで構成される。なお、ゲートウェイ１０１は、プロセッサ（不図示）と、プロセッサに接続されたメモリとを少なくとも備え、プロセッサがメモリを用いて所定のプログラムを実行することで下記の機能を実現する。

【００５３】

通信部１００５は、車載ネットワーク内に流れるメッセージの通信処理を行う通信インタフェースである。通信部１００５は、メッセージを受信すると、受信したメッセージをメッセージ処理部１００３又はコンテンツ検証部１００１に送信する。また、通信部１００５は、受信した車載ネットワークの任意のバスのメッセージを、別のバスへ転送する。

30

【００５４】

コンテンツ検証部１００１は、ＩＴＳ、又は、車車間通信などの車外のネットワーク経由で受信した自動車向けのコンテンツデータを検証する。

【００５５】

具体的には、コンテンツ検証部１００１は、コンテンツデータ、コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値、及び、複数の第一ハッシュ値と秘密鍵とを用いて生成された署名を取得する。コンテンツ検証部１００１は、車両１００aの状態を示す状態情報を取得する。コンテンツ検証部１００１は、複数の部分データのうち、取得した状態情報に応じて定められた所定数個の部分データのそれぞれから第二ハッシュ値を生成する。ここで所定数は１以上の整数である。コンテンツ検証部１００１は、生成した第二ハッシュ値と、複数の部分データのうちの所定数個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、署名とを用いて、取得したコンテンツデータの検証を行い、検証の結果を示す情報を出力する。

40

【００５６】

コンテンツ検証部１００１によるコンテンツデータの検証処理の詳細については後述する。

【００５７】

50

鍵保持部1002は、コンテンツ検証部1001又はメッセージ処理部1003が利用する鍵を保持する。具体的には、鍵保持部1002は、コンテンツ検証部1001がサーバ200から受信したコンテンツの検証に用いる鍵（つまり、サーバ200の公開鍵）を保持する。また、車載ネットワークがCANを含む場合、鍵保持部1002は、CANのメッセージに用いられるMAC（Message Authentication Code）の検証に用いる鍵（MAC鍵ともいう）を保持する。また、車載ネットワークがEthernet（登録商標）を含む場合、コンテンツ検証部1001は、Ethernet（登録商標）の暗号通信などに用いられる通信鍵を保持する。

【0058】

メッセージ処理部1003は、メッセージを処理する。例えば、車載ネットワークの任意のバス上のメッセージを別のバスに転送したり、メッセージの検証を行ったりする。メッセージ処理部1003は、鍵保持部1002に保持されているMAC鍵などの検証鍵を用いてメッセージの検証を行う。

【0059】

さらにメッセージ処理部1003は、メッセージから車両の状態を示す状態情報を取得し、車両状態保持部1004に保持する。状態情報は、例えば、車両100aが走行中であるか、停車中であるか、又は、駐車中であるかを示す走行状態情報を含む。車両100aが走行中であるか等は、トランスミッション120の情報又は速度情報から得られる。また、状態情報は、この処理を実行する装置であるゲートウェイ101の処理負荷を示す負荷情報を含んでもよいし、ゲートウェイ101が行う通信の通信量を示す通信量情報を含んでもよい。

【0060】

速度情報は、タイヤ（不図示）の回転数の情報を取得するECUから取得してもよいし、エンジン110に接続されているECU111、又は、ブレーキ130に接続されているECU131から取得してもよい。

【0061】

車両状態保持部1004は、車両の状態を保持する記憶装置である。車両状態保持部1004には、メッセージ処理部1003が取得した状態情報が格納される。また、車両状態保持部1004に格納された状態情報は、コンテンツ検証部1001により読み出される。

【0062】

1. 4 サーバ200の構成

図4は、本実施の形態におけるサーバ200の機能構成を示す模式図である。図4においてサーバ200は、コンテンツ収集部201、コンテンツDB202、コンテンツ分割部203、暗号処理部204、鍵保持部205、及び、通信部206を含んで構成される。なお、サーバ200は、プロセッサ（不図示）と、プロセッサに接続されたメモリとを少なくとも備え、プロセッサがメモリを用いて所定のプログラムを実行することで下記の機能を実現する。

【0063】

通信部206は、車両100a若しくは100b、又は、信号機300と通信を行う通信インタフェースである。通信部206は、通信プロトコルとして、TLS（Transport Layer Security）を用いてもよい。

【0064】

コンテンツ収集部201は、車両100a若しくは100b、又は、信号機300から取得したコンテンツデータを収集する。コンテンツデータには、車両100a若しくは100b又は信号機300から取得したセンサの情報、GPSなどにより取得された車両100a又は100bの位置情報、カメラにより取得された画像情報などが含まれ、これらのコンテンツデータから事故又は渋滞などの道路状況の把握がなされる。コンテンツ収集部201は、上記コンテンツデータとともに、当該コンテンツデータの更新間隔を示す指標を取得してもよい。

【0065】

コンテンツDB202は、コンテンツデータが記録される記録装置である。コンテンツDB202には、コンテンツ収集部201が収集したコンテンツデータが記録される。またコンテンツDB202は、地図データも記録する。コンテンツDB202が記録しているコンテンツデータは、コンテンツ分割部203により読み出される。

【0066】

コンテンツ分割部203は、コンテンツDB202に記録されているコンテンツデータの中から、車両100aの周辺の道路状況に対応するコンテンツデータを読み出し、分割を行う。車両100aの周辺の道路状況に対応するコンテンツデータを読み出す際には、コンテンツDB202に記録されているコンテンツデータの中から、別途取得する車両100aの位置情報に示される位置の周囲に対応するコンテンツデータを読み出す。そして、コンテンツ分割部203は、分割したコンテンツデータを暗号処理部204に送信する。なお、コンテンツデータが分割されたデータのそれぞれを部分データともいう。

10

【0067】

コンテンツ分割部203におけるコンテンツデータの分割の方法は、さまざまな方法があり得る。例えば、分割のサイズに関しては、分割後の部分データのサイズが一定値になるように分割してもよいし、コンテンツデータの種類ごとに分割するサイズを変更してもよい。

【0068】

鍵保持部205は、コンテンツデータの検証用データ生成に用いる秘密鍵（つまりサーバ200の秘密鍵）を保持する。

20

【0069】

暗号処理部204は、鍵保持部205が保持する秘密鍵を用いて、コンテンツデータの検証用データを生成する。暗号処理部204における検証用データの生成方法は後述する。

【0070】

なお、サーバ200は、インターネットに接続されていれば、物理的にはどこに配置されていてもよい、いわゆるクラウドサーバにより実現され得る。サーバ200が提供するコンテンツデータは、クラウドで生成されたコンテンツデータということもできる。

【0071】

30

1. 5 信号機300の構成

図5は、本実施の形態における信号機300の機能構成を示す模式図である。図5において信号機300は、コンテンツ収集部301、コンテンツDB302、コンテンツ分割部303、暗号処理部304、鍵保持部305、コンテンツ送信部306、センサ情報収集部307、及び、通信部308を含んで構成される。なお、信号機300は、プロセッサ（不図示）と、プロセッサに接続されたメモリとを少なくとも備え、プロセッサがメモリを用いて所定のプログラムを実行することで下記の機能を実現する。なお、信号機300は、これらの機能のほか、交通信号機としての機能を備えている。

【0072】

コンテンツDB302は、コンテンツDB202と同じ構成であり、コンテンツ分割部303はコンテンツ分割部203と同じ構成であり、暗号処理部304は暗号処理部204と同じ構成であり、鍵保持部305は鍵保持部205と同じ構成であるため、これらの構成の説明は省略する。

40

【0073】

コンテンツ収集部301は、V2Xで車両100a又は100bから取得したセンサ情報をコンテンツDB302へ格納する。

【0074】

コンテンツ送信部306は、コンテンツDB302で記録しているコンテンツデータをサーバ200に送信する。

【0075】

50

センサ情報収集部 307 は、信号機 300 に設置されているセンサ（不図示）が生成したセンサ情報、又は、カメラ（不図示）が生成した画像情報を取得し、コンテンツ DB 302 へ格納する。

【0076】

通信部 308 は、サーバ 200 との通信、及び、V2X での車両 100a 又は 100b との通信を行う通信インタフェースである。

【0077】

1. 6 車両 100a とサーバ 200 との通信シーケンス

次に、車両 100a とサーバ 200 との通信、より具体的にはサーバ 200 から車両 100a へのコンテンツデータのダウンロードと、車両 100a におけるコンテンツデータの検証処理とについて説明する。本実施の形態では、車両 100a がサーバ 200 から地図データ等のコンテンツデータをダウンロードし、車線維持機能に利用する場合を一例として説明する。

10

【0078】

＜コンテンツデータのダウンロードの通信シーケンス＞

図 6 は、本実施の形態におけるサーバ 200 から車両 100a へコンテンツデータをダウンロードする処理を示すシーケンス図である。図 6 に示されるシーケンスでは、車両 100a がサーバ 200 からコンテンツデータをダウンロードし、ダウンロードしたコンテンツデータを検証する処理が示されている。

【0079】

20

ステップ S101 において、サーバ 200 は、コンテンツデータを生成する。

【0080】

ステップ S102 において、サーバ 200 は、コンテンツデータを車両 100a へ送信する。

【0081】

ステップ S103 において、車両 100a の ITS 装置 190 は、サーバ 200 から送信されたコンテンツデータをダウンロードし、ITS 装置 190 用の ECU 191 へ送信する。ITS 装置 190 用の ECU 191 は、受信したコンテンツデータをゲートウェイ 101 に送信することで転送する。

【0082】

30

ステップ S104 において、ゲートウェイ 101 は、受信したコンテンツデータに対して検証を実行する。

【0083】

ステップ S105 において、ステップ S104 での検証において、受信したコンテンツデータが正当であると判定された場合、ゲートウェイ 101 は、受信したコンテンツデータに対してメッセージを生成する。

【0084】

ステップ S106 において、ゲートウェイ 101 は、ステップ S105 で生成したメッセージを、車線維持装置 160 用の ECU 161 へを送信する。

【0085】

40

ステップ S107 において、車線維持装置 160 用の ECU 161 は、ゲートウェイ 101 から受信したメッセージをもとに車線維持機能に係る動作を実行する。

【0086】

＜コンテンツデータの生成（ステップ S101）＞

図 7 は、本実施の形態におけるサーバ 200 によるコンテンツデータを生成する処理を示すフローチャートである。図 7 に示されるフローチャートは、図 6 におけるステップ S101 の内容を詳細に示すものである。

【0087】

ステップ S201 において、サーバ 200 のコンテンツ分割部 203 は、コンテンツデータを送信する対象である車両 100a に適したコンテンツデータをコンテンツ DB 20

50

2から取得する。なお、ステップS201で取得するコンテンツデータを、後述する「検証可能なコンテンツデータ」と区別して、コンテンツデータ本体ということもある。

【0088】

ステップS202において、サーバ200のコンテンツ分割部203は、ステップS201で取得したコンテンツデータを分割し、複数の部分データを生成する。

【0089】

ステップS203において、サーバ200の暗号処理部204は、ステップS202で分割により生成した複数の部分データそれぞれに対してハッシュ値を生成することで、複数のハッシュ値を生成する。ハッシュ値を生成するために用いるハッシュ関数はコンテンツ検証システム10であらかじめ決められており、例えばSHA-256である。

10

【0090】

ステップS204において、サーバ200の暗号処理部204は、ステップS203で生成した複数のハッシュ値それぞれに対して、鍵保持部205が保持する秘密鍵を用いて署名を生成する。署名の生成には、例えば、非特許文献1にあるECDSA(Elliptic Curve Digital Signature Algorithm)を用いる。

【0091】

ステップS205において、サーバ200の暗号処理部204は、ステップS202で生成した部分データと、ステップS203で生成したハッシュ値と、ステップS204で生成した署名とを含む、検証可能なコンテンツデータを生成する。検証可能なコンテンツデータの生成について、図8を参照しながら詳しく説明する。

20

【0092】

図8は、本実施の形態における検証可能なコンテンツデータを生成する処理の説明図である。具体的には、上記ステップS202からS205までの処理が説明される。

【0093】

図8に示されるように、暗号処理部204は、コンテンツデータC1を5つの部分データC11、C12、C13、C14及びC15に分割する(ステップS202)。

【0094】

次に、暗号処理部204は、生成した部分データC11、C12、C13、C14及びC15のそれぞれに対してハッシュ値を生成する。具体的には、暗号処理部204は、部分データC11に対してハッシュ値H11を生成し、部分データC12に対してハッシュ値H12を生成し、部分データC13に対してハッシュ値H13を生成し、部分データC14に対してハッシュ値H14を生成し、部分データC15に対してハッシュ値H15を生成する(ステップS203)。ここで、ハッシュ値H11、H12、H13、H14及びH15を第一ハッシュ値ともいう。

30

【0095】

次に、暗号処理部204は、生成したハッシュ値H11、H12、H13、H14及びH15を結合し、鍵保持部205が保持するサーバ200の秘密鍵を用いて署名S1を生成する(ステップS204)。

【0096】

次に、暗号処理部204は、ハッシュ値H11、H12、H13、H14及びH15、並びに、署名S1を検証用データVとしてコンテンツデータC1に付加することにより、検証可能なコンテンツデータC2を生成する(ステップS205)。つまり、検証可能なコンテンツデータC2には、コンテンツデータC1と検証用データVとが含まれている。

40

【0097】

<コンテンツデータの検証(ステップS104)>

図9は、本実施の形態における車両100aによるコンテンツデータを検証する処理を示すフローチャートである。図9に示されるフローチャートは、図6におけるステップS104の内容を詳細に示すものである。

【0098】

50

ステップS301において、車両100aのコンテンツ検証部1001は、サーバ200からコンテンツデータをダウンロードにより取得する。取得するコンテンツデータは、上記における検証可能なコンテンツデータC2に相当するものであり、具体的には、コンテンツデータ本体、コンテンツデータ本体を分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値、及び、複数の第一ハッシュ値と秘密鍵とを用いて生成された署名を含んでいる。

【0099】

ステップS302において、車両100aのコンテンツ検証部1001は、車両100aの状態を示す状態情報を取得する。車両100aの状態情報は、車両状態保持部1004から取得され得る。

10

【0100】

ステップS303において、車両100aのコンテンツ検証部1001は、ステップS302で取得した状態情報に応じて所定数を定める。

【0101】

ステップS304において、車両100aのコンテンツ検証部1001は、ダウンロードしたコンテンツデータに含まれる部分データのうち、所定数の部分データを選択する。なお、所定数は、1以上の整数であり、Nと表記することもある。

【0102】

ステップS305において、車両100aのコンテンツ検証部1001は、ステップS304で選択した部分データそれぞれに対するハッシュ値を生成する。ハッシュ値を生成するために用いるハッシュ関数は、コンテンツ検証システム10であらかじめ決められている。

20

【0103】

ステップS306において、車両100aのコンテンツ検証部1001は、ステップS304で選択しなかった部分データそれぞれに対するハッシュ値を、ステップS301で受信したコンテンツデータの中の検証用データに含まれるハッシュ値から抜き出す。

【0104】

ステップS307において、車両100aのコンテンツ検証部1001は、ステップS304で選択した部分データそれぞれに対して生成したハッシュ値と、ステップS304で選択しなかった部分データそれぞれに対してステップS306で抜き出したハッシュ値と、コンテンツデータの検証用データに含まれる署名とを用いて、コンテンツデータの検証を行うことによって、コンテンツデータが正当であるか否かを判定する。コンテンツデータの検証の際には、サーバ200の公開鍵が用いられる。コンテンツデータが正当であると判定した場合（ステップS307でYes）には、ステップS308に進み、そうでない場合（ステップS307でNo）には、ステップS309に進む。

30

【0105】

ステップS308において、車両100aのコンテンツ検証部1001は、ステップS301でダウンロードしたコンテンツデータが正当なコンテンツデータであることを示す情報を出力する。

【0106】

40

ステップS309において、車両100aのコンテンツ検証部1001は、ステップS301でダウンロードしたコンテンツデータが正当でない、つまり不正なコンテンツデータであることを示す情報を出力する。なお、このとき、当該コンテンツデータを破棄してもよい。

【0107】

図10は、本実施の形態におけるコンテンツデータを検証する処理の説明図である。具体的には、上記ステップS302からS305までの処理が説明される。図10では、検証可能なコンテンツデータD1を検証する処理を説明する。なお、検証可能なコンテンツデータD1は、図8で生成した検証可能なコンテンツデータC2に相当する。

【0108】

50

図10において、検証可能なコンテンツデータD1は、5つの部分データD11、D12、D13、D14及びD15と、検証用データWとを含む。検証用データWには、サーバ200が算出したハッシュ値J11、J12、J13、J14及びJ15と、署名T1とが含まれている。

【0109】

車両100aのコンテンツ検証部1001は、5つの部分データのうち所定数の部分データを選択する。ここでは、所定数を2とし、2つの部分データD11及びD13を選択する（ステップS302）。

【0110】

次に、選択した部分データD11に対してハッシュ値J21を生成し、部分データD13に対してハッシュ値J23を生成する（ステップS303）。ここで、ハッシュ値J21及びJ23を第二ハッシュ値ともいう。

10

【0111】

また、選択しなかった部分データD12、D14及びD15に対するハッシュ値を、検証可能なコンテンツデータD1の検証用データWから抜き出す（ステップS304）。ここでは、部分データD12に対してハッシュ値J12を抽出し、部分データD14に対してハッシュ値J14を抽出し、部分データD15に対するハッシュ値J15を抽出する。

【0112】

次に、ハッシュ値J21、J12、J23、J14及びJ15と、検証用データWに含まれる署名T1とを用いて、コンテンツデータD1の検証を行う（ステップS305）。

20

【0113】

なお、ステップS302で所定数個の部分データを選択する際には、複数の部分データから所定数個の部分データをランダムに選択してもよい。その場合、ステップS303では、選択した所定数個の部分データのそれぞれからハッシュ値J23等を生成する。このようにすることで、複数の部分データのうちのどの部分データを検証に使用するかが毎回変化するので、成りすましなどによる悪意あるデータをより適切に検出することができる。

【0114】

なお、ステップS303で所定数を定めるときには、走行状態情報を参照して、車両100aが走行中である場合には、所定数を第1の値に定め、車両100aが走行中でない場合には、所定数を第1の値より大きい第2の値に定めてもよい。言い換えれば、所定数は、車両状態保持部1004に保持された状態情報に応じて、可変であってもよい。例えば、状態情報（より具体的には走行状態情報）が「走行中」でない、つまり、「駐車中」又は「停車中」であれば、車両100aの状態が「走行中」の場合よりも、コンテンツデータを検証する時間を長く確保できるので、「走行中」の場合よりも所定数を大きくしてもよい。より具体的には、状態情報が「駐車中」又は「停車中」であれば、部分データの全数の3割を所定数とし、状態情報が「走行中」であれば、部分データの全数の1割を所定数としてもよい。このようにすることで、検証のために確保できる時間が比較的長い場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる時間が比較的短い場合には、短時間でコンテンツデータの検証を終えて、コンテンツ

30

40

【0115】

なお、ステップS303で所定数を定めるときには、この処理を実行する装置であるゲートウェイ101の負荷情報を参照して、処理負荷が高いほど、所定数をより小さな値に定めてもよい。また、ゲートウェイ101の通信量情報を参照し、通信量がより多いほど、所定数をより小さな値に定めてもよい。このようにすることで、検証のために確保できる処理能力が比較的大きい場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる処理能力が比較的小さい場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる利点がある。

【0116】

50

なお、ステップ S 3 0 3 で所定数を定めるときには、コンテンツデータの種類またはサイズに応じて所定数を定めてもよい。このようにすることで、コンテンツデータの種類またはサイズに適した所定数の部分データを検証に用いることができる。

【0117】

なお、ステップ S 3 0 3 で所定数を定めるときには、コンテンツデータの種類に基づいて、複数の部分データのうちのどの部分データを所定数個の部分データとして選択するかを決定してもよい。コンテンツデータの種類に応じて、どの部分データにどのような内容のデータが含まれているかが既知である場合には、検証の必要性がより高い部分を検証の対象とすることができる。

【0118】

なお、コンテンツデータの種類は、コンテンツデータの更新の間隔を示す指標を含んでもよい。このようにすることで、コンテンツデータの更新の時間間隔を具体的に用いてコンテンツの種類を示すことができる。

【0119】

＜車両 1 0 0 a からサーバ 2 0 0 へセンサ情報をアップロードするシーケンス＞

図 1 1 は、本実施の形態における車両 1 0 0 a からサーバ 2 0 0 へセンサ情報をアップロードする処理を示すシーケンス図である。

【0120】

ステップ S 4 0 1 において、車両 1 0 0 a のセンサを持つ E C U はセンサ情報を生成する。例えば、センサは、可視光により撮像するカメラ、又は、ミリ波レーダーである。

【0121】

ステップ S 4 0 2 において、車両 1 0 0 a の E C U からゲートウェイ 1 0 1 にセンサ情報を送信する。

【0122】

ステップ S 4 0 3 において、車両 1 0 0 a のゲートウェイ 1 0 1 は、E C U 1 9 1 へセンサ情報を転送する。

【0123】

ステップ S 4 0 4 において、E C U 1 9 1 は I T S 装置 1 9 0 から取得したセンサ情報をサーバ 2 0 0 へ送信（アップロード）する。

【0124】

ステップ S 4 0 5 において、サーバ 2 0 0 は、車両 1 0 0 a からセンサ情報を受信し、コンテンツ D B 2 0 2 に記録する。

【0125】

＜信号機 3 0 0 からサーバ 2 0 0 へセンサ情報をアップロードするシーケンス＞

図 1 2 は、本実施の形態における信号機 3 0 0 からサーバ 2 0 0 へセンサ情報をアップロードする処理を示すシーケンス図である。

【0126】

ステップ S 5 0 1 において、センサ情報収集部 3 0 7 は、センサ情報を生成する。センサ情報は、例えば、信号機 3 0 0 の周辺の道路状況、又は、信号機 3 0 0 の周辺のカメラの画像情報などである。

【0127】

ステップ S 5 0 2 において、センサ情報収集部 3 0 7 は、センサ情報をコンテンツ D B 3 0 2 に送信する。

【0128】

ステップ S 5 0 3 において、コンテンツ D B 3 0 2 は、センサ情報を記録する。

【0129】

ステップ S 5 0 4 において、コンテンツ送信部 3 0 6 は、コンテンツ D B 3 0 2 に記録されているセンサ情報を取得するために、コンテンツ D B 3 0 2 へアクセスし、センサ情報を取得する。

【0130】

10

20

30

40

50

ステップS505において、コンテンツ送信部306は、サーバ200へセンサ情報をアップロードする。

【0131】

ステップS506において、サーバ200は、信号機300からセンサ情報を受信し、コンテンツDB202にセンサ情報を記録する。

【0132】

1.7 実施の形態の効果

本実施の形態の検証方法によれば、検証装置つまりゲートウェイ101が、地図情報などを含む大容量のコンテンツデータを検証する場合に、コンテンツデータのうちの、車両の状態に応じて選択される一部を検証に用いるので、実用的なレベルで安全性を維持したまま、高速な検証が可能となり、安全なシステムの構築が可能となる。

10

【0133】

また、攻撃者は秘密鍵を持っておらず、攻撃者が正当な署名を生成することは困難であるので、検証装置は、コンテンツデータの検証用データに含まれる署名を用いて、コンテンツデータが正当であるか否かを検証でき、すなわち、攻撃者によるコンテンツデータの改ざんを検出できる。検証装置は、このようにコンテンツデータが正当であるか否かを検証できるので、その後に不正なコンテンツデータを破棄するなどして、車両の自動運転などの動作に正当なコンテンツデータのみを利用することによって、安全なシステムが構築できる。このように、検証装置は、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

20

【0134】

また、検証装置は、地図情報などを含む大容量のコンテンツデータを検証する場合に、コンテンツデータの一部をランダムに選択して検証するので、実用的なレベルで安全性を維持したまま、高速な検証が可能となり、安全なシステムの構築が可能となる。

【0135】

ここで、車両におけるコンテンツデータの検証は、コンテンツデータを複数に分割した部分データのうち所定数をランダムに選択してなされる。そのため、システムへの攻撃者が、コンテンツデータを不正に改ざんした場合、選択した分割されたコンテンツデータの中に攻撃者による不正な改ざんが含まれる可能性が高い。よって、検証装置は、コンテンツデータが正当であるか否かをより適切に検証できるので、より安全なシステムが構築できる。

30

【0136】

言い換えれば、検証装置が、複数の部分データのうちのどの部分データを検証に使用するか毎回変化するので、成りすましなどによる悪意あるデータをより適切に検出することができる。よって、検証装置は、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【0137】

また、検証装置は、検証のために確保できる時間が比較的長い場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる時間が比較的短い場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる時間の長短に応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

40

【0138】

また、検証装置は、検証のために確保できる処理能力が比較的大きい場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる処理能力が比較的小さい場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる処理能力の大小に応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【0139】

50

また、検証装置は、通信量情報から得られる、検証のために確保できる処理能力が比較的大きい場合には、コンテンツデータをより詳しく検証することができ、一方、検証のために確保できる処理能力が比較的小さい場合には、短時間でコンテンツデータの検証を終えて、コンテンツデータを利用できる。よって、検証装置は、検証のために確保できる処理能力の大小に応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【0140】

また、検証装置は、コンテンツデータの種類またはサイズに適した所定数の部分データを検証に用いることができる。よって、検証装置は、コンテンツデータの種類またはサイズに応じて、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

10

【0141】

また、検証装置は、コンテンツデータの種類に応じて、どの部分データにどのような内容のデータが含まれているかが既知である場合には、検証の必要性がより高い部分を検証の対象とすることができる。よって、検証装置は、検証の必要性がより高い部分を検証に用いることにより、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

【0142】

また、検証装置は、コンテンツデータの更新の時間間隔を用いてコンテンツの種類を示し、車両の自動運転への利用に、より適したコンテンツの検証方法により、コンテンツを検証できる。

20

【0143】

2. その他変形例

なお、本発明を上記実施の形態に基づいて説明してきたが、本発明は、上記実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【0144】

(1) 上記の実施の形態では、車載ネットワークはCANまたはEthernet（登録商標）またはCANとEthernet（登録商標）の混在であるとして説明したが、これに限定されることなく、例えば、CAN-FD（CAN with Flexible Data Rate）、LIN（Local Interconnect Network）、FlexRay（登録商標）であってもよいし、それぞれを組み合わせた構成であってもよい。

30

【0145】

(2) 上記の実施の形態では、車載ネットワークに送信されたメッセージからトランスミッションに係るギアの情報や速度情報を取得し、車両の状態を示す状態情報を取得したが、これに限定されない。車載カメラの画像情報、GPS、ミリ波レーダーやレーザーレーダーの情報やこれらを組み合わせて状態情報を推定してもよい。例えば、車載カメラの画像情報から車両の周囲の状況から、車両が、「走行中」、「駐車中」及び「停車中」のいずれであるかを判断してもよい。

【0146】

40

(3) 上記の実施の形態では、コンテンツデータから所定数の部分データを選択し、選択した部分データのそれぞれに対してハッシュ値を生成したが、所定数は状態情報だけでなく、取得したコンテンツデータの種類やサイズによって所定数を変更してもよい。コンテンツデータのサイズが比較的少ない場合は全ての分割されたコンテンツデータを選択すれば、コンテンツデータすべてに対して検証できる。

【0147】

(4) 上記の実施の形態では、コンテンツデータから分割されたコンテンツデータをランダムに選択したが、取得したコンテンツデータの種類によって、分割されたコンテンツデータの選択方法を変えてもよい。例えば、コンテンツデータが地図データの場合、車両の位置に近い地図データを含むように分割されたコンテンツデータを選択してもよいし、

50

地図データのうち、前に取得した分割されたコンテンツデータに対して差分の分割されたコンテンツデータを選択してもよい。また、地図データがダイナミックマップのように、静的な情報に動的な情報が重畳されている場合、動的情報を多く含むように分割されたコンテンツデータを選択してもよい。前回受信したコンテンツデータから差分の大きい分割されたコンテンツデータを積極的に選択することで、効率よくコンテンツデータを検証することができる。

【0148】

(5) 上記の実施の形態では、コンテンツデータの検証用データに署名を用いたが、これに限らない。車両がサーバや信号機と共通の秘密鍵を保持している場合、コンテンツデータのMAC (Message Authentication Code) を検証用データとしてもよい。このとき、MACはCMACやHMACを用いるとしてもよい。

10

【0149】

(6) 上記の実施の形態では、コンテンツデータのハッシュ値に対して署名を生成したが、これに限らない。複数の部分データのそれぞれのハッシュ値を結合し、結合したハッシュ値に対して、さらにハッシュ値を生成して、このハッシュ値に対して署名を生成してもよい。これにより、署名を生成する対象のハッシュ値が短くなり、署名が効率よく生成できる。

【0150】

(7) 上記の実施の形態における各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。RAMまたはハードディスクユニットには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、各装置は、その機能を達成する。ここでコンピュータプログラムは、所定の機能を達成するために、コンピュータに対する指令を示す命令コードが複数個組み合わせられて構成されたものである。

20

【0151】

(8) 上記の実施の形態における各装置は、構成する構成要素の一部または全部は、1個のシステムLSI (Large Scale Integration: 大規模集積回路) から構成されているとしてもよい。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAMなどを含んで構成されるコンピュータシステムである。RAMには、コンピュータプログラムが記録されている。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、システムLSIは、その機能を達成する。

30

【0152】

また、上記の各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又はすべてを含むように1チップ化されてもよい。

【0153】

また、ここでは、システムLSIとしたが、集積度の違いにより、IC、LSI、スーパーLSI、ウルトラLSIと呼称されることもある。また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA (Field Programmable Gate Array) や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

40

【0154】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

【0155】

(9) 上記の各装置を構成する構成要素の一部または全部は、各装置に脱着可能なICカードまたは単体のモジュールから構成されているとしてもよい。ICカードまたはモジ

50

ジュールは、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。ICカードまたはモジュールは、上記の超多機能LSIを含むとしてもよい。マイクロプロセッサが、コンピュータプログラムにしたがって動作することにより、ICカードまたはモジュールは、その機能を達成する。このICカードまたはこのモジュールは、耐タンパ性を有するとしてもよい。

【0156】

(10) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0157】

また、本発明は、コンピュータプログラムまたはデジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blue-ray (登録商標) Disc)、半導体メモリなどに記録したものとしてもよい。また、これらの記録媒体に記録されている前記デジタル信号であるとしてもよい。

【0158】

また、本発明は、コンピュータプログラムまたはデジタル信号を、電気通信回線、無線または有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしてもよい。

【0159】

また、本発明は、マイクロプロセッサとメモリを備えたコンピュータシステムであって、メモリは、コンピュータプログラムを記録しており、マイクロプロセッサは、コンピュータプログラムにしたがって動作するとしてもよい。

【0160】

また、プログラムまたはデジタル信号を前記記録媒体に記録して移送することにより、またはプログラムまたはデジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0161】

(11) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0162】

なお、上記各実施の形態において、各構成要素は、専用のハードウェアで構成されるか、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、CPUまたはプロセッサなどのプログラム実行部が、ハードディスクまたは半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。ここで、上記各実施の形態の検証装置などを実現するソフトウェアは、次のようなプログラムである。

【0163】

すなわち、このプログラムは、コンピュータに、車両で利用されるコンテンツデータを検証する検証方法であって、前記コンテンツデータと、前記コンテンツデータを分割した複数の部分データのそれぞれから生成された複数の第一ハッシュ値と、前記複数の第一ハッシュ値及び秘密鍵を用いて生成された署名とを取得し、前記車両の状態を示す状態情報を取得し、取得した前記状態情報に応じて1以上の整数であるNを定め、前記複数の部分データのうち前記N個の部分データのそれぞれから第二ハッシュ値を生成し、(a) 取得した前記複数の第一ハッシュ値のうち、前記複数の部分データのうちの前記N個の部分データを除く部分データのそれぞれから生成された第一ハッシュ値と、(b) 生成した前記第二ハッシュ値と、(c) 取得した前記署名と、を用いて、前記コンテンツデータの検証を行い、前記検証の結果を示す情報を出力する検証方法を実行させる。

【0164】

以上、一つまたは複数の態様に係る検証装置などについて、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しな

10

20

30

40

50

い限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

【産業上の利用可能性】

【0165】

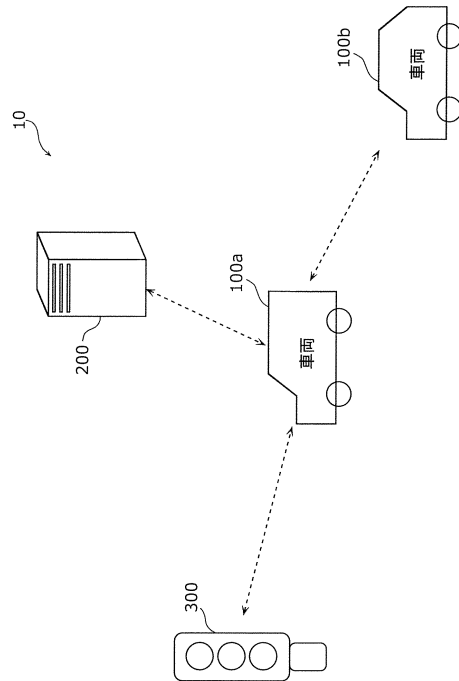
本発明は、地図情報などの大容量のコンテンツデータのダウンロードにおいて、コンテンツの一部をランダムに選んで検証することで、安全性を実用的なレベルで維持したまま、効率よく検証できる。これにより、安全なシステムを構築することが可能となる。

【符号の説明】

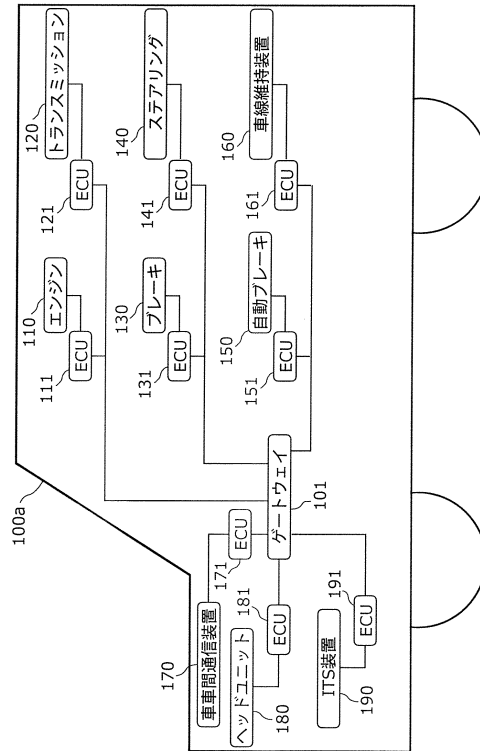
【0166】

10	コンテンツ検証システム	10
100a、100b	車両	
101	ゲートウェイ	
110	エンジン	
120	トランスミッション	
130	ブレーキ	
140	ステアリング	
150	自動ブレーキ	
160	車線維持装置	
170	車車間通信装置	20
180	ヘッドユニット	
190	ITS装置	
111、121、131、141、151、161、171、181、191	ECU	
200	サーバ	
201、301	コンテンツ収集部	
202、302	コンテンツDB	
203、303	コンテンツ分割部	
204、304	暗号処理部	
205、305、1002	鍵保持部	
206、308、1005	通信部	30
300	信号機	
306	コンテンツ送信部	
307	センサ情報収集部	
1001	コンテンツ検証部	
1003	メッセージ処理部	
1004	車両状態保持部	
C1、C2、D1	コンテンツデータ	
C11、C12、C13、C14、C15、D11、D12、D13、D14、D15	部分データ	
H11、H12、H13、H14、H15、J11、J12、J13、J14、J15		40
J21、J23	ハッシュ値	
S1、T1	署名	
V、W	検証用データ	

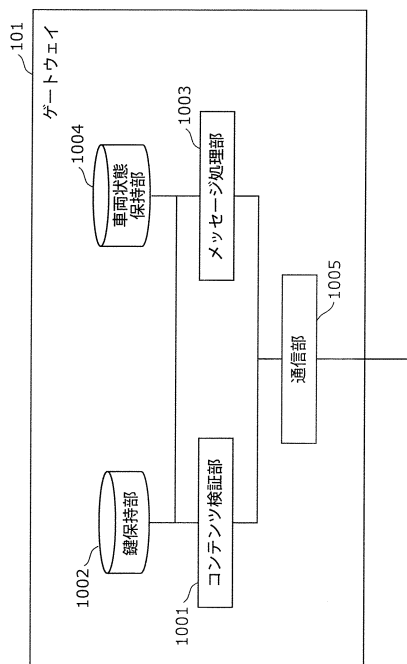
【図 1】



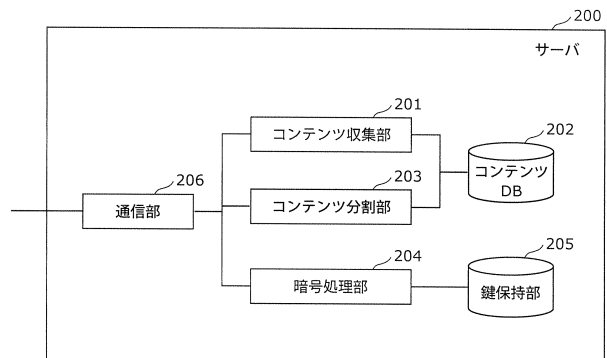
【図 2】



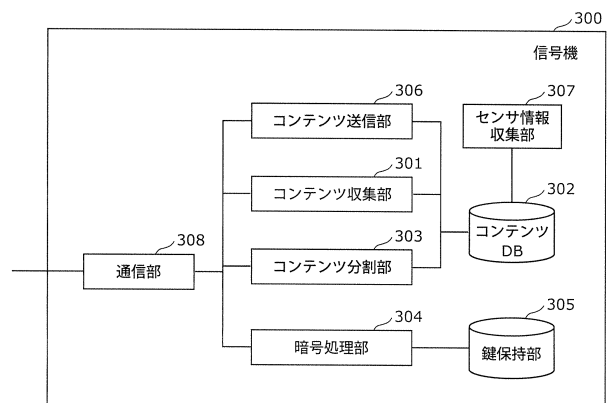
【図 3】



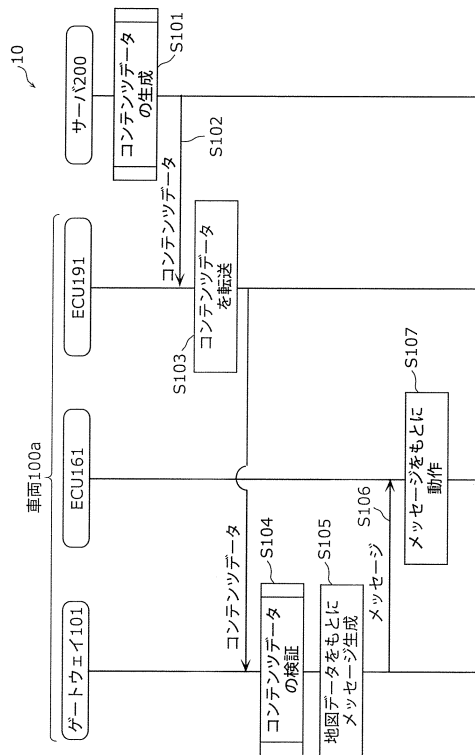
【図 4】



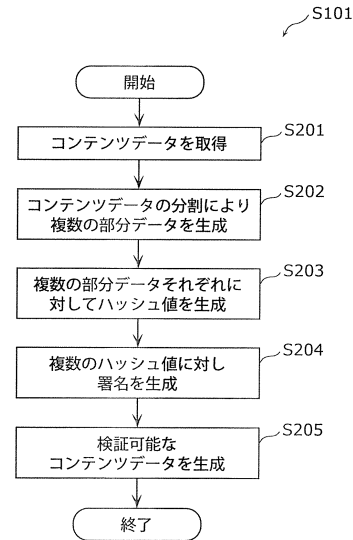
【図 5】



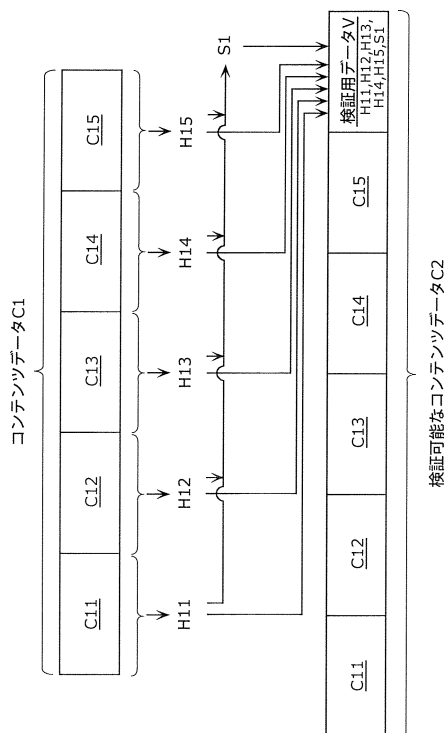
【図 6】



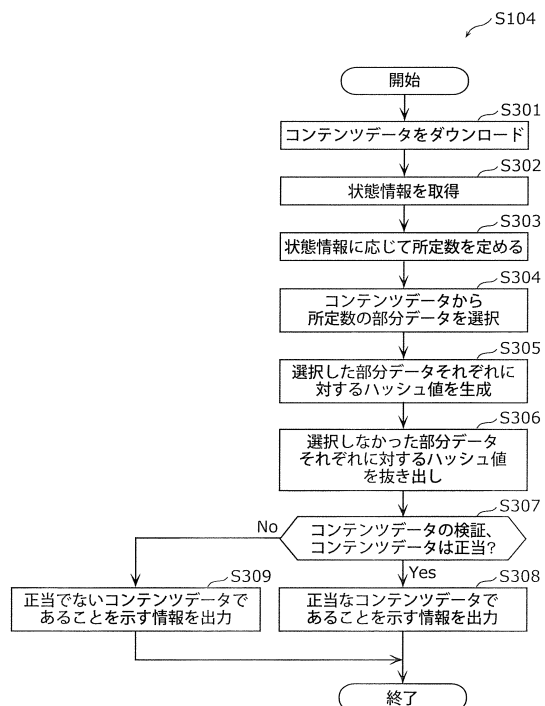
【図 7】



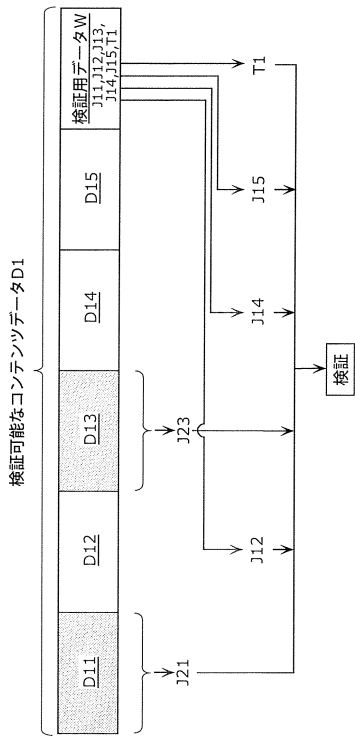
【图 8】



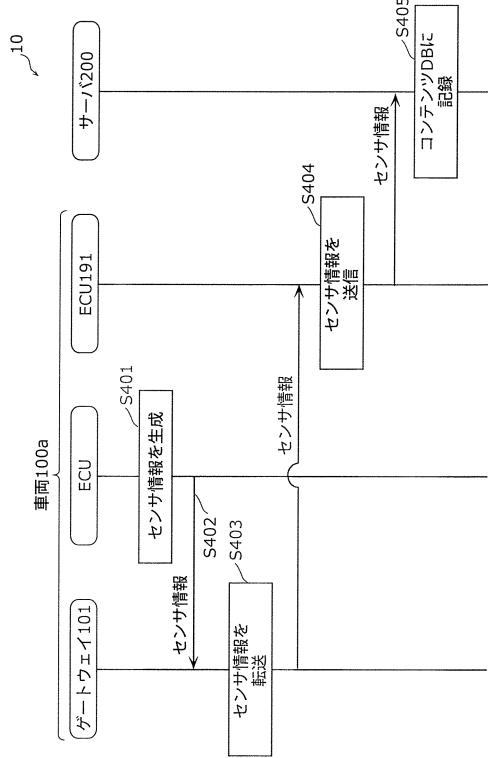
【图 9】



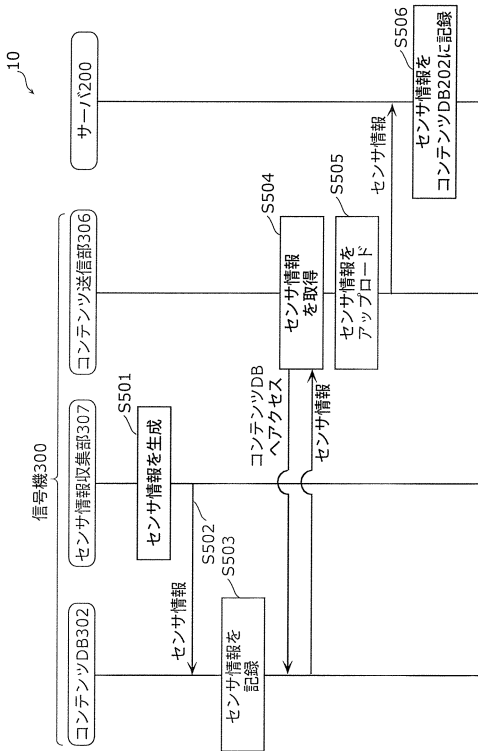
【図 1 0】



【図 1 1】



【図 1 2】



フロントページの続き

- (74)代理人 100131417
弁理士 道坂 伸一
- (72)発明者 海上 勇二
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 前田 学
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 芳賀 智之
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 松島 秀樹
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 安齋 潤
大阪府門真市大字門真1006番地 パナソニック株式会社内

審査官 金木 陽一

- (56)参考文献 特表2007-535189 (JP, A)
特開2014-14012 (JP, A)
国際公開第2016/075869 (WO, A1)
国際公開第2015/170452 (WO, A1)
特開2011-229076 (JP, A)
特表2016-534629 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04L 9/32
G06F 21/64