

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5429282号
(P5429282)

(45) 発行日 平成26年2月26日(2014.2.26)

(24) 登録日 平成25年12月13日(2013.12.13)

(51) Int.Cl.		F I		
G06F 21/62	(2013.01)	G06F 21/24	163E	
G06Q 10/00	(2012.01)	G06Q 10/00		
G06Q 50/00	(2012.01)	G06Q 50/00		

請求項の数 48 (全 25 頁)

(21) 出願番号	特願2011-506021 (P2011-506021)	(73) 特許権者	000004237
(86) (22) 出願日	平成22年3月15日 (2010.3.15)		日本電気株式会社
(86) 国際出願番号	PCT/JP2010/054760		東京都港区芝五丁目7番1号
(87) 国際公開番号	W02010/110193	(74) 代理人	100109313
(87) 国際公開日	平成22年9月30日 (2010.9.30)		弁理士 机 昌彦
審査請求日	平成25年2月18日 (2013.2.18)	(74) 代理人	100124154
(31) 優先権主張番号	特願2009-71217 (P2009-71217)		弁理士 下坂 直樹
(32) 優先日	平成21年3月24日 (2009.3.24)	(72) 発明者	山崎 健太郎
(33) 優先権主張国	日本国(JP)		東京都港区芝五丁目7番1号
			日本電気株式会社内
		審査官	矢頭 尚之

最終頁に続く

(54) 【発明の名称】 情報共有装置、情報共有方法、プログラム及び情報共有システム

(57) 【特許請求の範囲】

【請求項1】

情報収集手段と、

少なくとも第1の情報及び第2の情報を記憶する可搬型記憶装置と、

証明付取得要求生成手段と、

証明付取得要求処理手段とを含み、

前記情報収集手段は、前記可搬型記憶装置から前記第1の情報及び前記第2の情報を収集し、

前記証明付取得要求生成手段は、前記第2の情報の少なくとも一部からなる証明情報を含む証明付取得要求を送信し、

前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記第1の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

ことを特徴とする情報共有システム。

【請求項2】

前記証明情報は、前記可搬型記憶装置の固有識別子を含む

ことを特徴とする請求項1記載の情報共有システム。

【請求項3】

前記証明情報は、前記第2の情報に含まれる前記第2の情報の情報発生時刻を含み、

10

20

前記証明付取得要求処理手段は、前記情報発生時刻が前記第1の情報に含まれる計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

ことを特徴とする請求項1または2記載の情報共有システム。

【請求項4】

前記証明情報は、前記第2の情報に含まれる前記第2の情報の計測開始時刻と前記第2の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第2の情報に含まれる計測値とを含み、

前記証明付取得要求処理手段は、前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第1の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

10

ことを特徴とする請求項1乃至3のいずれかに記載の情報共有システム。

【請求項5】

前記証明情報は、前記第2の情報に含まれる前記第2の情報の計測開始時刻と前記第2の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第2の情報に含まれる計測値の非可逆要約とを含み、

前記証明付取得要求処理手段は、前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第1の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

20

ことを特徴とする請求項1乃至4のいずれかに記載の情報共有システム。

【請求項6】

前記証明付取得要求生成手段は、取得対象である前記第1の情報を特定する識別子である取得識別子をさらに含む証明付取得要求を送信し、

前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記証明付取得要求に含まれる取得識別子に対応する第1の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

30

ことを特徴とする請求項1記載情報共有システム。

【請求項7】

前記識別子は、前記可搬型記憶装置の固有識別子である

ことを特徴とする請求項6記載の情報共有システム。

【請求項8】

前記証明情報は、前記識別子である

ことを特徴とする請求項7記載の情報共有システム。

【請求項9】

前記証明情報は、前記第2の情報に含まれる前記第2の情報の情報発生時刻を含み、

前記証明付取得要求処理手段は、前記情報発生時刻が前記証明付取得要求に含まれる取得識別子に対応する前記第1の情報に含まれる前記第1の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第1の情報を送信するか否かを判定する

40

ことを特徴とする請求項6乃至8のいずれかに記載の情報共有システム。

【請求項10】

前記証明情報は、前記第2の情報に含まれる前記第2の情報の計測開始時刻と前記第2の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第2の情報に含まれる計測値とを含み、

50

前記証明付取得要求処理手段は、前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第 1 の情報を送信するか否かを判定する

ことを特徴とする請求項 6 乃至 9 のいずれかに記載の情報共有システム。

【請求項 1 1】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

10

前記証明付取得要求処理手段は、前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第 1 の情報を送信するか否かを判定する

ことを特徴とする請求項 6 乃至 1 0 のいずれかに記載の情報共有システム。

【請求項 1 2】

前記非可逆要約は、前記計測値のハッシュ値である

ことを特徴とする請求項 5 または 1 1 記載の情報共有システム。

【請求項 1 3】

20

可搬型記憶装置から第 1 の情報を収集する情報収集手段と、

前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する証明付取得要求処理手段と

を有することを特徴とする情報共有装置。

【請求項 1 4】

前記証明情報は、前記可搬型記憶装置の固有識別子である

ことを特徴とする請求項 1 3 記載の情報共有装置。

30

【請求項 1 5】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、

前記証明付取得要求処理手段は、前記情報発生時刻が前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 1 3 または 1 4 記載の情報共有装置。

【請求項 1 6】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、

40

前記証明付取得要求処理手段は、前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 1 3 乃至 1 5 のいずれかに記載の情報共有装置。

【請求項 1 7】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

50

前記証明付取得要求処理手段は、前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 13 至 16 のいずれかに記載の情報共有装置。

【請求項 18】

前記証明付取得要求は、取得対象である前記第 1 の情報を特定する識別子をさらに含み、

前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記識別子で特定される前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に第 1 の情報を送信するか否かを判定する、
ことを特徴とする請求項 13 記載の情報共有装置。

【請求項 19】

前記識別子は、前記可搬型記憶装置の固有識別子である

ことを特徴とする請求項 18 記載の情報共有装置。

【請求項 20】

前記証明情報は、前記識別子である

ことを特徴とする請求項 19 記載の情報共有装置。

【請求項 21】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、

前記証明付取得要求処理手段は、前記情報発生時刻が前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 18 乃至 20 のいずれかに記載の情報共有装置。

【請求項 22】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、

前記証明付取得要求処理手段は、前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 18 乃至 21 のいずれかに記載の情報共有装置。

【請求項 23】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

前記証明付取得要求処理手段は、前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する、

ことを特徴とする請求項 18 乃至 22 のいずれかに記載の情報共有装置。

【請求項 24】

前記非可逆要約は、前記計測値のハッシュ値である

ことを特徴とする請求項 17 または 23 記載の情報共有装置。

【請求項 25】

可搬型記憶装置から第 1 の情報を収集し、

前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明

10

20

30

40

50

情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定することを特徴とする情報共有方法。

【請求項 2 6】

前記証明情報は、前記可搬型記憶装置の固有識別子であることを特徴とする請求項 2 5 記載の情報共有方法。

【請求項 2 7】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、前記情報発生時刻が前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定することを特徴とする請求項 2 5 または 2 6 記載の情報共有方法。

10

【請求項 2 8】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定することを特徴とする請求項 2 5 乃至 2 7 のいずれかに記載の情報共有方法。

20

【請求項 2 9】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定することを特徴とする請求項 2 5 乃至 2 8 のいずれかに記載の情報共有方法。

30

【請求項 3 0】

前記証明付取得要求は、取得対象である前記第 1 の情報を特定する識別子をさらに含み、前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記識別子で特定される前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に第 1 の情報を送信するか否かを判定することを特徴とする請求項 2 5 記載の情報共有方法。

【請求項 3 1】

前記識別子は、前記可搬型記憶装置の固有識別子であることを特徴とする請求項 3 0 記載の情報共有方法。

40

【請求項 3 2】

前記証明情報は、前記識別子であることを特徴とする請求項 3 1 記載の情報共有方法。

【請求項 3 3】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、前記情報発生時刻が前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送

50

信するか否かを判定すること

を特徴とする請求項 30 乃至 32 のいずれかに記載の情報共有方法。

【請求項 34】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、

前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定すること

10

を特徴とする請求項 30 乃至 33 のいずれかに記載の情報共有方法。

【請求項 35】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定すること

を特徴とする請求項 30 乃至 34 のいずれかに記載の情報共有方法。

20

【請求項 36】

前記非可逆要約は、前記計測値のハッシュ値であること

を特徴とする請求項 29 または 35 記載の情報共有方法。

【請求項 37】

可搬型記憶装置から第 1 の情報を収集し、

前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

をコンピュータに実行させることを特徴とするプログラム。

30

【請求項 38】

前記証明情報は、前記可搬型記憶装置の固有識別子であること

を特徴とする請求項 37 記載のプログラム。

【請求項 39】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、

前記情報発生時刻が前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

をコンピュータに実行させることを特徴とする請求項 37 または 28 記載のプログラム

40

【請求項 40】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、

前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

をコンピュータに実行させることを特徴とする請求項 37 乃至 39 のいずれかに記載のプログラム。

50

【請求項 4 1】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

をコンピュータに実行させることを特徴とする請求項 3 7 乃至 4 0 のいずれかに記載のプログラム。

10

【請求項 4 2】

前記証明付取得要求は、取得対象である前記第 1 の情報を特定する識別子をさらに含み、

前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記識別子で特定される前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に第 1 の情報を送信するか否かを判定する処理

をコンピュータに実行させることを特徴とする請求項 3 7 記載のプログラム。

【請求項 4 3】

前記識別子は、前記可搬型記憶装置の固有識別子であること

を特徴とする請求項 4 2 記載のプログラム。

20

【請求項 4 4】

前記証明情報は、前記識別子であること

を特徴とする請求項 4 3 記載のプログラム。

【請求項 4 5】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の情報発生時刻を含み、

前記情報発生時刻が前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる前記第 1 の情報の計測開始時刻と計測終了時刻との間のいずれかの時刻に一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

30

をコンピュータに実行させることを特徴とする請求項 4 2 乃至 4 4 のいずれかに記載のプログラム。

【請求項 4 6】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値とを含み、

前記証明情報に含まれる計測値と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

40

をコンピュータに実行させることを特徴とする請求項 4 2 乃至 4 5 のいずれかに記載のプログラム。

【請求項 4 7】

前記証明情報は、前記第 2 の情報に含まれる前記第 2 の情報の計測開始時刻と前記第 2 の情報の計測終了時刻と当該計測開始時刻及び当該計測終了時刻の間の時刻における前記第 2 の情報に含まれる計測値の非可逆要約とを含み、

前記証明情報に含まれる非可逆要約と、前記証明情報に含まれる計測開始時刻及び計測終了時刻の間の時刻における前記証明付取得要求に含まれる取得識別子に対応する前記第 1 の情報に含まれる計測値の非可逆要約とが一致するか否かを検査した結果に基づいて、証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理

50

をコンピュータに実行させることを特徴とする請求項 4 2 乃至 4 6 のいずれかに記載のプログラム。

【請求項 4 8】

前記非可逆要約は、前記計測値のハッシュ値であることを特徴とする請求項 4 1 または 4 7 記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報共有装置、情報共有方法、プログラム及び情報共有システムに関し、特に情報へのアクセス制御を行う情報共有装置、情報共有方法、プログラム及び情報共有システムに関する。

10

【背景技術】

【0002】

非特許文献 1 に記載された E P C I S (E l e c t r o n i c P r o d u c t C o d e s I n f o r m a t i o n S e r v i c e s) に代表されるような物品についての情報運用においては、各企業により管理されるデータサーバが、在庫情報や出庫情報などの物流情報の収集を行う。そしてさらに、これらの物流情報を共有するシステムにおいては、これらの物流情報に対するアクセス制御が行われる。

例えば、アクセス制御システムの 1 例が特許文献 1 に記載されている。特許文献 1 のアクセス制御システムは、アクセスの可否を判断するための専用の情報をポリシーエンジンのポリシー格納手段及びアクセス制御装置のアクセス制御リスト格納手段にて管理する。

20

また、無線タグシステムの 1 例が特許文献 2 に記載されている。特許文献 2 の無線タグシステムは、アクセスの可否を判断するための専用の情報を外部記憶装置の D B にて管理する。

また、製品の流通履歴の検索方法の 1 例が特許文献 3 に記載されている。特許文献 3 の製品の流通履歴の検索方法は、識別子を付与した製品情報、製品流通経路の業者情報及び製品経路のトレースデータをデータベースに格納し、それぞれの識別子を用いて相互に検索する構成を有する。この構成により、特許文献 3 の製品の流通履歴の検索方法は、トレースデータ間の追跡を可能とする技術を提供する。

また、商品管理システムの 1 例が特許文献 4 に記載されている。特許文献 4 の商品管理システムは、商品に付された無線タグに記憶された商品 I D (I D e n t i f i e r) と流通データとに基づいて、データサーバに収集された商品流通経路の各施設の温度データから対象の商品が存在した時刻の温度データを抽出する。続けて、特許文献 4 の商品管理システムは、合成して温度履歴データを生成する。

30

また、物流管理システムの 1 例が特許文献 5 に記載されている。特許文献 5 の物流管理システムは、物流対象物に付与した R F I D (R a d i o F r e q u e n c y I D e n t i f i c a t i o n) タグに識別子、通過時刻及び通過地点情報を 1 つの流通イベントコードとして保存する構成を有する。さらに、特許文献 5 の物流管理システムは、流通イベント集計サーバが流通イベントコードを収集し、集計保存し、要求に応じて提供する構成を有する。こうして特許文献 5 の物流管理システムは、クライアントが履歴情報を取得することを可能とする。

40

また、トレースシステムの 1 例が特許文献 6 に記載されている。特許文献 6 のトレースシステムは、流通経路情報の登録用の認証コードの生成及び検証にタグ I D (I D e n t i f i c a t i o n) を含む情報のハッシュを用いている。

【先行技術文献】

【特許文献】

【0003】

【特許文献 1】特開 2 0 0 6 - 0 5 3 8 2 4 号公報

【特許文献 2】特開 2 0 0 6 - 1 8 5 1 1 6 号公報

【特許文献 3】特開 2 0 0 5 - 1 0 0 3 2 5 号公報

50

【特許文献4】特開2004-299827号公報

【特許文献5】特開2005-234628号公報

【特許文献6】特開2008-265940号公報

【非特許文献】

【0004】

【非特許文献1】EPCglobal Inc., The EPCglobal Architecture Framework Version 1.2、2007年9月 (http://www.epcglobalinc.org/standards/architecture/architecture__1__2-framework-20070910.pdf)

10

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、上述した先行技術文献に記載された技術においては、アクセス制御のためのアクセスルールを設定及び管理する負担が大きいという問題点がある。

例えば、品物に取り付けられたセンサタグで収集した物流過程での温度、湿度、衝撃などの履歴といった物流情報は、企業にとって重要なデータであるため、誰にでも開示してよいものではない。

そのため、個々の物流情報について、どの企業に対して開示するかあるいはしないかということ制御するためのアクセスルールを設定する必要がある。

20

しかし、新たな物流情報が収集されるたびに、その物流情報に対するアクセスルールの設定を行うことは、その設定を行うユーザあるいはシステムにとって大きな負担となる。

具体的に、上述した先行技術文献に記載された技術を用いて特定の品物の物流情報をその品物の物流に関わる複数の企業間で共有しようとした場合に負担が大きくなる理由を以下に説明する。まず、システムはアクセスの可否を判断するためだけに利用する情報（アクセスルール）として、物流情報と前記物流情報にアクセス可能な企業（ユーザ）の識別子との対応表を管理することとなる。

ところが、一般的に物流業界では、ある品物の物流に関わる企業の1つを取り上げたとき、その企業がその品物の物流に関わる他の全ての企業を知っているとは限らない。多くの場合、その企業が知っている他の企業は、その企業と直接の取引関係がある企業のみである。

30

例えば、A社がB社を利用してX社へ品物を運送する場合に、B社は実運送業務をC社、D社に委託するということが考えられる。この場合、A社は運送がB社からC社、D社に委託されていることを必ずしも認識しないということ、またC社、D社は運送を請け負った品物がA社のものであることを知らないということが起こり得る。

このような物流業界の特性から、品物の物流に関わる企業の識別子を事前に全て得ることは容易ではなく、アクセスルールを設定することには困難が伴う。

即ち、上述した先行技術文献に記載されたような、共有したい情報とは別に、データサーバ管理者がアクセスルールを作成、管理するシステムや方法では、データサーバ管理者の負担が大きい。

40

本発明の目的は、上述した課題を解決する情報共有装置、情報共有方法、プログラム及び情報共有システムを提供することにある。

【課題を解決するための手段】

【0006】

本発明の情報共有システムは、情報収集手段と、

少なくとも第1の情報及び第2の情報を記憶する可搬型記憶装置と

証明付取得要求生成手段と、

証明付取得要求処理手段とを含み、

前記情報収集手段は、前記可搬型記憶装置から前記第1の情報及び前記第2の情報を収集し、

50

前記証明付取得要求生成手段は、前記第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を送信し、

前記証明付取得要求処理手段は、受信した前記証明付取得要求に含まれる前記証明情報が、前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元の証明付取得要求生成手段を搭載している装置に前記第 1 の情報を送信するか否かを判定する。

本発明の情報共有装置は、可搬型記憶装置から第 1 の情報を収集する情報収集手段と、前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する証明付取得要求処理手段とを有する。

10

本発明の情報共有方法は、可搬型記憶装置から第 1 の情報を収集し、前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する。

本発明のプログラムは、可搬型記憶装置から第 1 の情報を収集し、前記可搬型記憶装置から収集した情報である第 2 の情報の少なくとも一部からなる証明情報を含む証明付取得要求を受信した場合に、受信した当該証明付取得要求に含まれる証明情報が前記第 1 の情報のいずれかの部分に一致するか否かを検査した結果に基づいて、前記証明付取得要求の送信元に前記第 1 の情報を送信するか否かを判定する処理をコンピュータに実行させる。

20

【発明の効果】

【0007】

本発明の効果は、特定の品物の物流情報をこの品物の物流に関わる複数のデータサーバ間でのみ共有するアクセス制御のためのアクセスルールを設定及び管理する負担を軽減することを可能にできることである。

【図面の簡単な説明】

【0008】

30

【図 1】本発明の第 1 の実施形態の構成を示すブロック図である。

【図 2】本発明の第 1 及び第 5 の実施形態の物流情報の構造を示す図である。

【図 3】本発明の第 1 及び第 5 の実施形態の証明付取得要求の構造を示す図である。

【図 4】本発明の第 1 ～ 第 4 の実施形態の一連の動作を示すフローチャートである。

【図 5】本発明の第 1 ～ 第 4 の実施形態の要求処理の動作を示すフローチャートである。

【図 6】本発明の第 1 ～ 第 4 の実施形態の応答処理の動作を示すフローチャートである。

【図 7】本発明の第 2 の実施形態の物流情報の構造を示す図である。

【図 8】本発明の第 2 の実施形態の証明付取得要求の構造を示す図である。

【図 9】本発明の第 3 及び第 4 の実施形態の物流情報の構造を示す図である。

【図 10】本発明の第 3 の実施形態の証明付取得要求の構造を示す図である。

40

【図 11】本発明の第 4 の実施形態の証明付取得要求の構造を示す図である。

【図 12】本発明の第 5 の実施形態の構成を示すブロック図である。

【発明を実施するための形態】

【0009】

次に、本発明の実施形態について図面を参照して詳細に説明する。

図 1 を参照すると、本発明の第 1 の実施形態に係るトレーサビリティシステムは、入出力装置 100、可搬型記憶装置 200、物流情報収集装置（情報収集手段とも呼ばれる）300、物流情報アドレス解決装置 400、データサーバ 500 とから構成されている。

物流情報アドレス解決装置 400 とデータサーバ 500 とは、互いにネットワークを介して接続されている。

50

入出力装置 100 は、例えば、データサーバ 500 に接続されたマウスやキーボード等の入力装置、ディスプレイ等の出力装置、CPU (Central Processing Unit)、メモリ及びハードディスク装置などを備えた一般的なサーバ装置やパーソナルコンピュータ、あるいは、携帯端末上で動作するプログラムで実現される。

入出力装置 100 は、物流情報 600 (第2の情報及び第1の情報とも呼ばれる。詳細は後述) を特定する品物の識別子を入力装置やプログラムから入力されると、この品物の識別子を含む取得要求を証明付取得要求生成部 530 に送信する機能を有する。更に、入出力装置 100 は、証明付取得要求生成部 530 から物流情報 600 を受信して出力装置への表示や対応するプログラムの実行などの機能を有する。

可搬型記憶装置 200 は、自身を識別させるための識別子である固有識別子 620 を保持する機能と、データを記憶する機能と、物流情報収集装置 300 及び物流設備 (図示しない) と通信を行う機能とを有する。可搬型記憶装置 200 は、例えばRFIDタグや携帯端末で実現される。また、可搬型記憶装置 200 は、センサー付きタグなどであって、温度、湿度あるいは衝撃などの環境情報を収集する機能を備えていてもよい。

可搬型記憶装置 200 は、例えば、物流状態情報 (例えば、入庫や出庫などのイベントのステップ、イベントの発生した時刻、などの情報)、物流状態情報を受信した場所、可搬型記憶装置 200 の位置情報及び環境情報などを物流情報 600 に対応する内容として記憶する。尚、環境情報は、例えば、可搬型記憶装置 200 自身で収集したあるいは物流施設から受け取った、温度情報、湿度情報あるいは衝撃情報などである。また、可搬型記憶装置 200 は、固有識別子 620 及び記憶している物流情報 600 に対応する内容を物流情報収集装置 300 へ送信する。

物流情報収集装置 300 (情報収集装置とも呼ばれる) は、可搬型記憶装置 200 と通信を行う機能と、データサーバ 500 と通信を行う機能とを有する。物流情報収集装置 300 は、例えば、RFIDタグと情報をやり取りするRFIDリーダなどのデバイスで実現される。もしくは、物流情報収集装置 300 は、そのようなデバイスを接続した、CPU、メモリ、ハードディスク装置などを備えた一般的なサーバ装置やパーソナルコンピュータと、デバイスが収集したデータの加工を行うRFIDミドルウェアといったプログラムとの組み合わせで実現される。また、例えば、データサーバ 500 が、このようなデバイスを接続され、RFIDミドルウェアを搭載される構成としてもよい。

物流情報収集装置 300 は、可搬型記憶装置 200 から固有識別子 620 などの情報を収集する機能を有する。さらに、物流情報収集装置 300 は、収集した情報から少なくとも固有識別子 620 を含む物流情報 600 を作成する機能を有する。さらに、物流情報収集装置 300 は、作成した物流情報 600 をデータサーバ 500 の物流情報記憶部 510 に送る機能を有する。

物流情報 600 は、図2に示すように、少なくとも固有識別子 620 を含み、さらにイベント時刻 630、イベントステップ 640、読み取り場所 650 及びタグの存在場所 660 のうち1つ以上を含んでもよい。尚、「<」及び「>」とこれらで囲まれた文字列は、デリミタ (delimiter) である (以下、他の図も同様)。また、イベント時刻 630 は、例えばイベントの発生した時刻の情報であり、情報発生時刻とも呼ばれる。また、イベントステップ 640 は、例えば、入庫や出庫などの情報である。また、読み取り場所 650 は、例えば、物流状態情報を受信した場所の情報であり、タグの存在場所 660 は、例えば、可搬型記憶装置 200 の位置の情報である。またさらに、物流情報 600 は、物流過程における複数の環境情報 (例えば、温度情報、湿度情報あるいは衝撃情報) の履歴情報のうち1つ以上を含んでもよい。

物流情報アドレス解決装置 400 は、ONS (Object Name Service) やP2P (Peer to Peer) などのアドレス解決を行う技術を用いたプログラム、もしくはこれらのような機能を有する一般的なサーバ装置やパーソナルコンピュータでもよい。また、このプログラムをデータサーバ 500 上に置くことにより、データサーバ 500 が物流情報アドレス解決装置 400 を含む構成としてもよい。

物流情報アドレス解決装置 400 は、証明付取得要求 700 (詳細は後述) を証明付取

10

20

30

40

50

得要求生成部 530 から受信する機能を有する。さらに、物流情報アドレス解決装置 400 は、受信した証明付取得要求 700 を、この証明付取得要求 700 に含まれる取得識別子 710 に対応する物流情報 600 を保持する物流情報記憶部 510 を有するデータサーバ 500 の証明付取得要求処理部 540 へ、送信する機能を有する。尚、取得識別子 710 は、後述する証明付取得要求生成部 530 によって、品物の識別子に対応させたものである。

データサーバ 500 は、物流情報記憶部 510、証明付取得要求生成部 530、証明付取得要求処理部 540 及び通信部 520 を有する。

物流情報記憶部 510 は、物流情報収集装置 300 から受信した 1 以上の物流情報 600 を記憶する。また、物流情報記憶部 510 は、証明付取得要求生成部 530 または証明付取得要求処理部 540 からの要求に対応して物流情報 600 を提供する。

通信部 520 は、インターネット、LAN (Local Area Network) などのネットワークを利用してデータの送受信を行う機能を有する。

証明付取得要求生成部 530、証明付取得要求処理部 540 及び物流情報アドレス解決装置 400 間における証明付取得要求 700 及び物流情報 600 の送受信は、本通信部 520 を介して実現される。尚、以下の説明においては、通信部 520 を介して通信を行うことの記載は省略する。

証明付取得要求生成部 530 は、入出力装置 100 から取得要求を受信する機能と、取得要求に含まれる品物の識別子に対応する物流情報 600 を物流情報記憶部 510 に要求して物流情報 600 を取得する機能とを有する。さらに、証明付取得要求生成部 530 は、取得した物流情報 600 から証明物流情報 (証明情報とも呼ばれる) 790 を作成する機能を有する。さらに、証明付取得要求生成部 530 は、取得要求に含まれる品物の識別子を取得識別子 710 とし、この取得識別子 710 と証明物流情報 790 とを含む図 3 に示すような証明付取得要求 700 を作成する機能を有する。さらに、証明付取得要求生成部 530 は、作成した証明付取得要求 700 を物流情報アドレス解決装置 400 に送信する機能と、証明付取得要求 700 に対する応答である物流情報 600 を受信する機能とを有する。

証明付取得要求処理部 540 は、物流情報アドレス解決装置 400 から証明付取得要求 700 を受信する機能と、証明付取得要求 700 に含まれる取得識別子 710 に対応する物流情報 600 を物流情報記憶部 510 に要求して物流情報 600 を取得する機能と、取得した物流情報 600 の内容 (例えば、固有識別子 620) と証明付取得要求 700 に含まれる証明物流情報 790 の内容 (例えば、固有識別子 720) とを比較する機能と、比較した結果に基づいて取得した物流情報 600 に対するアクセス可否を判定する機能と、アクセス可であると判定をした場合に、取得した物流情報 600 を証明付取得要求 700 の送信元のデータサーバ 500 に送信する機能とを有する。

次に、本実施形態の動作について図 1 ~ 図 6 を参照して詳細に説明する。

まず、各装置間にまたがるトレーサビリティシステムの動作を説明する。図 4 は、データサーバ 500 が他データサーバ 500 から物流情報 600 を取得する一連の動作を示すフローチャートである。

まず、操作者が、入出力装置 100 から品物の識別子を含む取得要求を入力することにより動作が開始される (S101)。

入出力装置 100 は、取得要求をデータサーバ 500 の証明付取得要求生成部 530 に送る (S102)。

次に、証明付取得要求生成部 530 は、入出力装置 100 から受け取った取得要求に含まれる品物の識別子に対応する物流情報 600 (第 2 の情報) を自データサーバ 500 の物流情報記憶部 510 に要求し、取得する。そして、証明付取得要求生成部 530 は、取得要求に含まれる品物の識別子を取得識別子 710 とし、取得識別子 710 と取得した物流情報 600 から作成した証明物流情報 790 (第 2 の情報の一部を含む) とを含む証明付取得要求 700 を生成する (S103)。

尚、S103 において、取得識別子 710 に対応する物流情報 600 が自データサーバ

10

20

30

40

50

500の物流情報記憶部510に存在しない場合、証明付取得要求生成部530は、証明物流情報790を含まない証明付取得要求700を生成してもよい。あるいは、証明付取得要求生成部530は、証明付取得要求700を作成せずに他データサーバ500の物流情報600の取得動作を終了するようにしてもよい。

続けて、証明付取得要求生成部530は、物流情報アドレス解決装置400に証明付取得要求700を送信する(S104)。尚、以下の説明において、この証明付取得要求700を送信した証明付取得要求生成部530のデータサーバ500を取得要求元(証明付取得要求の送信元とも呼ばれる)と呼ぶ。

次に、物流情報アドレス解決装置400は、証明付取得要求700に含まれる取得識別子710に対応する物流情報600(第1の情報)を保持している他のデータサーバ500を特定し、当該データサーバ500に証明付取得要求700を転送する(S105)。

10

次に、物流情報アドレス解決装置400から前記証明付取得要求700を受けた他のデータサーバ500の証明付取得要求処理部540は、証明付取得要求700に含まれる取得識別子710に対応する物流情報600を物流情報記憶部510から取得する(S106)。

続けて、証明付取得要求処理部540は、物流情報記憶部510から取得した物流情報600(第1の情報)と証明付取得要求700に含まれる証明物流情報790(第2の情報の一部を含む)とに基づき、この取得した物流情報600に対する取得要求元のアクセス権の有無を判定する(S107)。アクセス権有と判定した場合(S107でYES)、証明付取得要求処理部540は、物流情報記憶部510から取得した物流情報600を取得要求元へ送信する(S108)。アクセス権無しと判定した場合(S107でNO)、取得要求元への物流情報600の送信は行わないで、処理は終了する。

20

尚、アクセス権無しと判定されるのは、証明付取得要求700に証明物流情報790が含まれない場合や、証明物流情報790が捏造されたものであると判断した場合である。また、捏造の判断は、取得した物流情報600に含まれる固有識別子620、イベント時刻630、イベントステップ640、読み取り場所650及びタグの存在場所660と、これらにそれぞれ対応する証明物流情報790に含まれる固有識別子720、イベント時刻730、イベントステップ740、読み取り場所750及びタグの存在場所760との内少なくとも1組を比較することで実行する。

上述した本実施形態のトレーサビリティシステムにおけるデータサーバ500が他データサーバ500から物流情報600を取得する一連の動作で実行する処理は、大きくは証明付取得要求700を作成し送信する要求処理と、受信した証明付取得要求700を処理する応答処理とに分けることができる。

30

そこで次に、本実施形態の証明付取得要求700を作成し送信する要求処理の動作について、より詳細に説明する。図4は本実施形態における、要求処理の動作を示すフローチャートである。

証明付取得要求生成部530は、品物の識別子を含む取得要求を、入出力装置100から受信する(S201)。

続けて、証明付取得要求生成部530は、取得要求に含まれる品物の識別子に基づいて物流情報600を物流情報記憶部510に要求する(S202)。

40

次に、物流情報記憶部510は、保持している物流情報600の内から取得要求に含まれる品物の識別子を含む物流情報600を検索し、存在した場合は検索された物流情報600を証明付取得要求生成部530に返す。また、存在しなかった場合、物流情報記憶部510は、エラー情報もしくは空の物流情報600を証明付取得要求生成部530に返す(S203)。

次に、証明付取得要求生成部530は、物流情報記憶部510から取得した情報が期待した物流情報600であるか否かを判定し(S204)、物流情報600である場合(S204でYES)、処理はS205に進む。また、エラーである場合(S204でNO)、処理は終了する。

S205において、証明付取得要求生成部530は、S203で受信した物流情報600

50

0に基づいて、証明物流情報790を作成する(S205)。本実施の形態の例では、図2に示すような物流情報600に含まれる固有識別子620「urn:id:xxx...」イベント時刻630「2008-12-01T080031」、イベントステップ640「arrival」、読み取り場所650「loc01」及びタグの存在場所660「loc02」をそれぞれ、固有識別子720「urn:id:xxx...」イベント時刻730「2008-12-01T080031」、イベントステップ740「arrival」、読み取り場所750「loc01」及びタグの存在場所760「loc02」としたものを含む図3に示すような証明物流情報790を作成する。

続けて、証明付取得要求生成部530は、S201で受信した取得要求に含まれる品物の識別子を取得識別子710とし、これとS205において作成した証明物流情報790とを含む証明付取得要求700を作成する(S206)。

10

続けて、証明付取得要求生成部530は、物流情報アドレス解決装置400に証明付取得要求700を送信する(S207)。

続けて、証明付取得要求生成部530は、受信待機の状態になり、他データサーバ500からの証明付取得要求700に対する応答を待つ(S208)。そして、応答を受信した場合(S208でYES)、処理はS209に進み、所定の時間を経過しても応答を受信しなかった場合(S208でNO)、処理は終了する。

S209において、証明付取得要求生成部530は、入出力装置100にS208で受信した他データサーバ500からの応答である物流情報600もしくはエラーを出力する。

20

以上説明したように、S201からS208の動作により、証明付取得要求生成部530は、取得識別子710に対応した自データサーバ500の物流情報600を含む証明付取得要求700を作成、送信する。そして、S209からS210の動作により、証明付取得要求生成部530は、他データサーバ500から前記証明付取得要求700に対する応答を受信する。

次に、本実施形態の証明付取得要求700を処理する応答処理の動作について、より詳細に説明する。図5は本実施形態における、応答処理の動作を示すフローチャートである。

証明付取得要求処理部540は、物流情報アドレス解決装置400から証明付取得要求700を受信する(S221)。

30

続けて、証明付取得要求処理部540は、受信した証明付取得要求700から取得識別子710を抽出し、この取得識別子710に対応する物流情報600を物流情報記憶部510に要求する(S222)。

次に、物流情報記憶部510は、保持している物流情報600の内から取得識別子710を含む物流情報600を検索し、存在した場合は検索された物流情報600を、存在しなかった場合はエラー情報を証明付取得要求処理部540に返す(S223)。

次に、証明付取得要求処理部540は、物流情報記憶部510から取得した情報が物流情報600であるかエラーであるか否かを判定し(S224)、物流情報600である場合(S224でYES)、処理はS225に進む。また、エラーである場合(S224でNO)、処理はS226へ進む。

40

次に、証明付取得要求処理部540は、証明付取得要求700に含まれる証明物流情報790から固有識別子720を抽出し、S223で取得した物流情報600から固有識別子620を抽出し、これらを比較する(S225)。そして固有識別子620と固有識別子720とが一致した場合(S225でYES)、証明付取得要求処理部540は、取得要求元にはこの取得した物流情報600に対するアクセス権があると判定し、処理はS226に進む。一致しない場合(S225でNO)、証明付取得要求処理部540は、取得要求元にはこの取得した物流情報600に対するアクセス権がないと判定し、処理は終了する。

S226において、証明付取得要求処理部540は、S223で物流情報記憶部510から取得した情報(即ち、物流情報600またはエラー)を取得要求元のデータサーバ5

50

00の証明付取得要求生成部530に送信する(S226)。

以上説明したように、証明付取得要求処理部540は、S205にて証明付取得要求生成部530が作成した証明付取得要求700に含まれる証明物流情報790(certification)の固有識別子720(id)を、S223にて取得した物流情報600の固有識別子620と一致するか否かを判定し、一致した場合にアクセス権があると判断する。

尚、本実施形態において、証明付取得要求生成部530と証明付取得要求処理部540間での証明付取得要求700の送受信は、物流情報アドレス解決装置400を介して行うように構成される例を示した。他の例として、送信先のデータサーバ500のアドレスが送信元のデータサーバ500にとって既知の場合には、物流情報アドレス解決装置400を介さず、直接送受信を行うように構成されてもよい。そして、この場合は、物流情報アドレス解決装置400が構成に含まれなくてもよい。

10

上述した本実施形態における第1の効果は、特定の品物の物流情報600をこの品物の物流に関わる複数のデータサーバ500間でのみ共有する場合に、そのためのアクセス制御を行うアクセスルールを設定及び管理する負担を軽減することができる点である。

その理由は、各データサーバ500が記憶している物流情報600を証明情報として、各データサーバ500間でのアクセス権の判定を行うように構成したからである。

上述した本実施形態における第2の効果は、特定の品物の物流情報600をこの品物の物流に関わる複数のデータサーバ500間でのみ共有する場合に、アクセス制御のためのアクセスルールを設定及び管理する負担をさらに軽減することができる点である。

20

その理由は、RFIDの物理IDを物流情報600の固有識別子620として使用するよう構成したからである。

上述した本実施形態における第3の効果は、アクセスルールの増大による物理的リソースの消費増加や、アクセス制御処理速度の低下を防止することを可能にできる点である。

その理由は、各データサーバ500が記憶している物流情報600のみを証明情報として、各データサーバ500間でのアクセス権の判定を行うように構成したためである。即ち、このように構成したので、データサーバ500が物流情報600以外を管理することもルールマッチ処理も必要なくなるためである。

上述した本実施形態における第4の効果は、アクセスの許可範囲を事前に設定することなしに、特定の品物の物流情報600をこの品物の物流に関わる複数のデータサーバ500間でのみ共有することを可能にできる点である。

30

その理由は、ユーザ識別子ではなく、各データサーバ500が記憶している物流情報600を証明情報として、各データサーバ500間でのアクセス権の判定を行うように構成したからである。

例えば、物流情報600の固有識別子620と証明物流情報790の固有識別子720が一致することをもってアクセス権があると判断するということは、取得要求元のデータサーバ500が固有識別子720を含む証明物流情報790を作成可能な物流情報600を保持していることを持って、取得要求元のデータサーバ500が当該物流情報600の品物の物流に関わるデータサーバ500であることを示していることと見做すということである。

40

こうして本実施の形態は、例えば取得要求元のデータサーバ500が取得識別子710で表される品物の物流に関わるデータサーバ500であるかどうかを判断し、物流に関わる企業のデータサーバ500のみが物流情報600にアクセス可能とする。

このように本実施の形態は、物流情報600をアクセス制御に利用することにより、アクセスユーザを示すユーザ識別子を利用することや物流情報600毎にアクセスルールを設定することなしに、特定の品物の物流情報600をその品物の物流に関わる複数のデータサーバ500のみで共有を可能にするアクセス制御を実現する。

次に、本発明の第2の実施形態に係るトレーサビリティシステムについて、図面を参照して詳細に説明する。

本発明の第2の実施形態に係るトレーサビリティシステムは、第1の実施形態に較べて

50

、物流情報600の構造、証明物流情報790を作成する動作及び受信した証明付取得要求700と物流情報600とを比較する動作が異なる。

本発明の第2の実施形態の物流情報600は、図7に示すように、固有識別子720とイベント時刻630とセンサデータ670とを少なくとも含む構造を有する。さらに、センサデータ670は、少なくとも計測開始時刻671及び計測終了時刻672を少なくとも含む。

本発明第2の実施形態の動作は、第1の実施形態の動作を示す図5のステップS205及び図6のステップS225が、以下に示すS305及びS425にそれぞれ置き換えられる。

S305において、証明付取得要求生成部530は、S203で受信した物流情報600に基づいて、証明物流情報790を作成する(S305)。本実施の形態の例では、図7に示すような物流情報600に含まれる固有識別子620「urn:id:xxx...」、イベント時刻630「2008-12-01T080031」、イベントステップ640「arrival」、読み取り場所650「loc01」、タグの存在場所660「loc02」、計測開始時刻671「2008-12-01T000023」及び計測終了時刻672「2008-12-01T080031」をそれぞれ、固有識別子720「urn:id:xxx...」、イベント時刻730「2008-12-01T080031」、イベントステップ740「arrival」、読み取り場所750「loc01」、タグの存在場所760「loc02」、計測開始時刻771「2008-12-01T000023」及び計測終了時刻772「2008-12-01T080031」としたものを含む図8に示すような証明物流情報790を作成する。

S425において、証明付取得要求処理部540は、証明付取得要求700に含まれる証明物流情報790から固有識別子720及びイベント時刻730を抽出する。続けて、証明付取得要求処理部540は、S223で取得した物流情報600から固有識別子620、計測開始時刻671及び計測終了時刻672を抽出する。更に続けて、証明付取得要求処理部540は、固有識別子720及びイベント時刻730と、固有識別子620、計測開始時刻671及び計測終了時刻672とを比較する(S425)。そして固有識別子620と固有識別子720とが一致し、かつイベント時刻730がS223で得た物流情報600のセンサデータ670の計測開始時刻671と計測終了時刻672との間の時刻であった場合(S425でYES)、証明付取得要求処理部540は、取得要求元にはこの取得した物流情報600に対するアクセス権があると判定し、処理はS226に進む。

また、固有識別子620と固有識別子720とが一致しない、またはイベント時刻730がS223で得た物流情報600のセンサデータ670の計測開始時刻671と計測終了時刻672との間の時刻でなかった場合(S425でNO)、証明付取得要求処理部540は、取得要求元にはこの取得した物流情報600に対するアクセス権がないと判断し、処理は終了する。

上述した本実施形態における効果は、第1の実施の形態の効果に加え、より厳格にアクセス権を判断することを可能にできる点である。

その理由は、固有識別子720に併せて、イベント時刻730を用いてアクセス権の判定を行うようにしたからである。

本実施形態の効果は、RFIDタグが再使用される場合にも有用である。

なぜならば、固有識別子720としてRFIDの物理識別子を使用している場合、RFIDタグが再使用された際に、2つ以上の品物の異なる物流情報600に対して同じ固有識別子620が振られる問題が生じる。そして、第1の実施例の形態によるトレーサビリティシステムでは、前記問題が生じた際に2つ以上の品物の異なる物流情報600の区別ができないため、証明物流情報790が異なる使用機会での物流情報600であったとしてもアクセス権ありと判断してしまう場合がありえる。

本実施形態をとることで、取得要求元のデータサーバ500が、取得対象である物流情報600に含まれる計測開始時刻671から計測終了時刻672の間にその物流情報600に対応する物流に関わったか否かを確認することができる。従って、取得要求元のデー

10

20

30

40

50

タサーバ500は、証明物流情報790が異なる使用機会での物流情報600であった場合にアクセス権なしと判断できる。

R F I Dタグが再使用され、2つ以上の異なる品物に取り付けられた場合において、物流情報記憶部510は、これらの品物を直接区別するための情報を保持しない。しかし、第2の実施例の形態をとることにより、特定の品物の物流に関わるデータサーバ500のみが、物流情報600にアクセスできるようにすることを実現している。

次に、本発明の第3の実施形態に係るトレーサビリティシステムについて、図面を参照して詳細に説明する。

本発明の第3の実施形態に係るトレーサビリティシステムは、第1の実施形態に較べて、物流情報600及び証明物流情報790の構造と、証明物流情報790を作成する動作及び受信した証明付取得要求700と物流情報600とを比較する動作とが異なる。

本発明の第3の実施形態の物流情報600は、図9に示すように、固有識別子620とイベント時刻630とセンサデータ670とを少なくとも含む構造を有する。さらに、センサデータ670は、計測開始時刻671、計測終了時刻672、計測間隔673及び計測値674を少なくとも含む。計測値674は、計測開始時刻671から計測間隔673毎に可搬型記憶装置200が物流設備から環境データとして取得した情報の集合である。従って、計測開始時刻671と計測間隔673と計測値674とに基づいて、計測値674に含まれる環境データ毎の計測時刻が算出できる。

本発明第3の実施形態の動作は、第1の実施形態の動作を示す図5のステップS205及び図6のステップS225が、以下に示すS505及びS625にそれぞれ置き換えられる。

S505において、証明付取得要求生成部530は、S203で受信した物流情報600に基づいて、証明物流情報790を作成する(S505)。本実施の形態の例では、図9に示すような物流情報600に含まれる固有識別子620「urn:id:xxx...」、イベント時刻630「2008-12-01T080031」、イベントステップ640「arrival」、読み取り場所650「loc01」、タグの存在場所660「loc02」、計測開始時刻671「2008-12-01T000023」、計測終了時刻672「2008-12-01T080031」、計測間隔673「600」及び計測値674「0A1A532C...」をそれぞれ、固有識別子720「urn:id:xxx...」、イベント時刻730「2008-12-01T080031」、イベントステップ740「arrival」、読み取り場所750「loc01」及びタグの存在場所760「loc02」、計測開始時刻771「2008-12-01T000023」、計測終了時刻772「2008-12-01T080031」、計測間隔773「600」及び計測値774「0A1A532C...」としたものを含む図10に示すような証明物流情報790を作成する。

従って、本発明の第3の実施形態の証明付取得要求700は、第1の実施形態の証明付取得要求700に比べて、証明物流情報790に少なくとも計測開始時刻771、計測終了時刻772、計測間隔773及び計測値774を含むセンサデータ770が追加されている。

S625において、証明付取得要求処理部540は、証明付取得要求700に含まれる証明物流情報790から固有識別子720及びセンサデータ770を抽出する。続けて、証明付取得要求処理部540は、S223で取得した物流情報600から固有識別子620及びセンサデータ670を抽出する。更に続けて、証明付取得要求処理部540は、固有識別子720及びセンサデータ770と、固有識別子620及びセンサデータ670とを比較する(S625)。そして固有識別子620と固有識別子720とが一致し、かつ計測値774に含まれる全ての環境データとその計測時刻との組の内容が、S223で得た物流情報600の計測値674に含まれる環境データとその計測時刻との組に一致した場合(S625でYES)、証明付取得要求処理部540は、取得要求元にはこの取得した物流情報600に対するアクセス権があると判定し、処理はS226に進む。また、固有識別子620と固有識別子720とが一致しない、または計測値774に含まれる環境

10

20

30

40

50

データとその計測時刻との組の内容の内の少なくとも1つが、S 2 2 3で得た物流情報6 0 0の計測値6 7 4に含まれる環境データとその計測時刻との組のいずれかに一致しなかった場合(S 6 2 5でNO)、証明付取得要求処理部5 4 0は、取得要求元にはこの取得した物流情報6 0 0に対するアクセス権がないと判断し、処理は終了する。

上述した本実施形態における第1の効果は、第1の実施の形態の効果に加え、より厳格にアクセス権を判断することを可能にできる点である。

その理由は、固有識別子7 2 0に併せて、センサデータ7 7 0を用いてアクセス権の判定を行うようにしたからである。

本実施形態の効果は、証明物流情報7 9 0となる物流情報6 0 0を悪意あるユーザが作成しようとした場合にも有効である。

即ち、第1、2の実施形態では、悪意を持ったユーザが時刻のみが正しいセンサデータ6 7 0を捏造し、アクセス権を取得する可能性がある。

本実施形態では、証明付取得要求処理部5 4 0は、取得要求元のデータサーバ5 0 0が取得識別子7 1 0で示される品物の物流に関連するデータサーバ5 0 0であるかどうかの判断を、センサデータ6 7 0の照合で行っている。

取得要求元のデータサーバ5 0 0が取得識別子7 1 0で示される品物の物流に関連するデータサーバ5 0 0であれば、このデータサーバ5 0 0は、可搬型記憶装置2 0 0がこのデータサーバ5 0 0を経由した際に物流情報収集装置3 0 0によりデータを収集する。従って、このデータサーバ5 0 0は、取得対象の物流情報6 0 0に含まれる計測値6 7 4の一部に完全に一致する物流情報6 0 0を持っている。従って、取得識別子7 1 0で示される品物の物流に関連するデータサーバ5 0 0は、これに基づいて証明物流情報7 9 0を作成できる。一方、悪意あるユーザが、取得対象の物流情報6 0 0に含まれる計測値6 7 4の一部に完全に一致するような証明物流情報7 9 0を作成することは困難である。

こうして、本実施形態は、悪意あるユーザによる証明物流情報7 9 0の捏造を防止し、特定の品物の物流に関わるデータサーバ5 0 0のみが対応する物流情報6 0 0にアクセスできるようにすることを実現している。

次に、本発明の第4の実施形態に係るトレーサビリティシステムについて、図面を参照して詳細に説明する。

本発明の第4の実施形態に係るトレーサビリティシステムは、第3の実施形態に較べて、証明物流情報7 9 0の構造と、証明物流情報7 9 0を作成する動作及び受信した証明付取得要求7 0 0と物流情報6 0 0とを比較する動作とが異なる。

本発明の第3の実施形態に係るトレーサビリティシステムは、証明付取得要求生成部5 3 0で作成する証明付取得要求7 0 0の証明物流情報7 9 0に含めるセンサデータ6 7 0として物流情報記憶部5 1 0から取得した計測開始時刻6 7 1、計測終了時刻6 7 2、計測間隔6 7 3及び計測値6 7 4をそのまま利用していた。しかし、本実施形態に係るトレーサビリティシステムは、計測間隔6 7 3及び計測値6 7 4に対して特定の演算を施して変換した、非可逆要約情報7 7 5を利用する。

この特定の演算は、例えば、一方向性ハッシュ関数などを利用して実現できる。

本発明第3の実施形態の動作は、第3の実施形態の動作のステップS 5 0 5及びステップS 6 2 5が、以下に示すS 7 0 5及びS 8 2 5にそれぞれ置き換えられる。

S 7 0 5において、証明付取得要求生成部5 3 0は、S 2 0 3で受信した物流情報6 0 0に基づいて、証明物流情報7 9 0を作成する(S 7 0 5)。本実施の形態の例では、図9に示すような物流情報6 0 0に含まれる固有識別子6 2 0「urn:id:xxx...」、イベント時刻6 3 0「2008-12-01T080031」、イベントステップ6 4 0「arrival」、読み取り場所6 5 0「loc01」、タグの存在場所6 6 0「loc02」、計測開始時刻6 7 1「2008-12-01T000023」、計測終了時刻6 7 2「2008-12-01T080031」、計測間隔6 7 3「600」及び計測値6 7 4「0A1A532C...」に基づいて、図11に示すような固有識別子7 2 0「urn:id:xxx...」、イベント時刻7 3 0「2008-12-01T080031」、イベントステップ7 4 0「arrival」、読み取り場所7 5 0「lo

10

20

30

40

50

c 0 1」、タグの存在場所 7 6 0「l o c 0 2」及び、計測開始時刻 7 7 1「2 0 0 8 - 1 2 - 0 1 T 0 0 0 2 3」と計測終了時刻 7 7 2「2 0 0 8 - 1 2 - 0 1 T 0 8 0 0 3 1」と非可逆要約情報 7 7 5「e 0 1 3 a c 2 . . .」を含むセンサデータ 7 7 0 を含む証明物流情報 7 9 0 を作成する。

S 8 2 5 において、証明付取得要求処理部 5 4 0 は、証明付取得要求 7 0 0 に含まれる証明物流情報 7 9 0 から固有識別子 7 2 0 及びセンサデータ 7 7 0 を抽出し、S 2 2 3 で取得した物流情報 6 0 0 から固有識別子 6 2 0 及びセンサデータ 6 7 0 を抽出する。続けて、証明付取得要求処理部 5 4 0 は、計測開始時刻 7 7 1 から計測終了時刻 7 7 2 までの時刻にあたる計測値 6 7 4 を抽出する。さらに続けて、証明付取得要求処理部 5 4 0 は、これらに対して S 7 0 5 で非可逆要約情報 7 7 5 を作成する場合と同様の特定の演算を施して非可逆要約情報 6 7 5 (図示しない) を作成する。さらに続けて、証明付取得要求処理部 5 4 0 は、固有識別子 7 2 0 及び非可逆要約情報 7 7 5 と固有識別子 6 2 0 及び非可逆要約情報 6 7 5 とを比較する (S 8 2 5) 。そして固有識別子 6 2 0 と固有識別子 7 2 0 とが一致し、かつ非可逆要約情報 6 7 5 と非可逆要約情報 7 7 5 とが一致した場合 (S 8 2 5 で Y E S) 、証明付取得要求処理部 5 4 0 は、取得要求元にはこの取得した物流情報 6 0 0 に対するアクセス権があると判定し、処理は S 2 2 6 に進む。また、固有識別子 6 2 0 と固有識別子 7 2 0 とが一致しなかった、または非可逆要約情報 6 7 5 と非可逆要約情報 7 7 5 とが一致しなかった場合 (S 8 2 5 で N O) 、証明付取得要求処理部 5 4 0 は、取得要求元にはこの取得した物流情報 6 0 0 に対するアクセス権がないと判断し、処理は終了する。

上述した本実施形態における第 1 の効果は、第 3 の実施形態の効果に加えて物流情報 6 0 0 のセキュリティを高めることができる点である。

その理由は、アクセス制御の対象である物流情報 6 0 0 を非可逆要約情報 7 7 5 に変換して、アクセス権有無の判定材料として利用するようにしたからである。

第 3 の実施形態の場合、証明付取得要求 7 0 0 は特別な保護を施されていない。従って、例えば、取得識別子 7 1 0 の品物の物流に関係のないデータサーバ 5 0 0 に証明付取得要求 7 0 0 を知られることは、証明物流情報 7 9 0 に含まれるセンサデータ 6 7 0 を知られてしまうことに直結する。

本実施形態では、証明付取得要求 7 0 0 に含まれるセンサデータ 6 7 0 の計測値 6 7 4 は非可逆要約情報 7 7 5 に変換されている。従って、取得識別子 7 1 0 の品物の物流に関係のないデータサーバ 5 0 0 に実際の計測値 6 7 4 を知られてしまうことを防ぐことができる。

上述した本実施形態における第 2 の効果は、証明付取得要求 7 0 0 のデータサイズを削減することができる点である。

その理由は、アクセス権有無の判定材料とする物流情報 6 0 0 を非可逆要約情報 7 7 5 に圧縮変換して利用するようにしたからである。

次に、本発明の第 5 の実施形態について図面を用いて詳細に説明する。

本実施形態は、本発明の基本的な要素からなる実施形態である。図 1 2 を参照すると、本発明の第 5 の実施形態は、物流情報収集装置 3 0 0 及び証明付取得要求処理部 5 4 0 とから構成されている。

物流情報収集装置 3 0 0 は、可搬型記憶装置 (図示しない) から情報を収集する。

証明付取得要求処理部 5 4 0 は、可搬型記憶装置から収集した物流情報 6 0 0 の少なくとも一部からなる証明物流情報 7 9 0 を含む証明付取得要求 7 0 0 を受信した場合に、受信した証明付取得要求 7 0 0 に含まれる証明物流情報 7 9 0 が、同じ可搬型記憶装置から収集した物流情報 6 0 0 のいずれかの部分に一致するか否かを検査する。続けて、証明付取得要求処理部 5 4 0 は、この検査した結果に基づいて、証明付取得要求 7 0 0 の送信元に物流情報 6 0 0 を送信するか否かを判定する。

上述した本実施形態における第 1 の効果は、特定の品物の物流情報 6 0 0 をこの品物の物流に関わる複数のデータサーバ 5 0 0 間でのみ共有するアクセス制御のためのアクセスルールを設定及び管理する負担を軽減することを可能にできる点である。その理由は、可

10

20

30

40

50

搬型記憶装置から収集した情報に基づいて、要求された情報の送信をするか否かを判定するようにしたからである。

以上の各実施形態で説明した各構成要素は、例えば、プログラムにより所定の処理をコンピュータに実行させてもよい。

以上の各実施形態で説明した各構成要素は、必ずしも個々に独立した存在である必要はなく、複数の構成要素が1個のモジュールとして実現されたり、1つの構成要素が複数のモジュールで実現されたり、ある構成要素が他の構成要素の一部であったり、ある構成要素の一部と他の構成要素の一部とが重複していたり、といったような構成であってもよい。

また、以上説明した各実施形態では、複数の動作をフローチャートの形式で順番に記載してあるが、その記載の順番は複数の動作を実行する順番を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の順番は内容的に支障のない範囲で変更することができる。

さらに、以上説明した各実施形態では、複数の動作は個々に相違するタイミングで実行されることに限定されない。例えば、ある動作の実行中に他の動作が発生したり、ある動作の実行タイミングと他の動作の実行タイミングとの一部乃至全部が重複していたりしてもよい。

さらに、以上説明した各実施形態では、ある動作が他の動作の契機になるように記載しているが、その記載はある動作と他の動作の全ての関係を限定するものではない。このため、各実施形態を実施するときには、その複数の動作の関係は内容的に支障しない範囲で変更することができる。また各構成要素の各動作の具体的な記載は、各構成要素の各動作を限定するものではない。このため、各構成要素の具体的な各動作は、各実施形態を実施する上で機能的、性能的、その他の特性に対して支障をきたさない範囲内で変更されてよい。

尚、以上説明した各実施形態における各構成要素は、必要に応じ可能であれば、ハードウェアで実現されてもよいし、ソフトウェアで実現されてもよいし、ハードウェアとソフトウェアの混在により実現されてもよい。

また、各構成要素の物理的な構成は、以上の実施形態の記載に限定されることはなく、独立して存在してもよいし、組み合わされて存在してもよいしまたは分離して構成されてもよい。

以上、実施形態（及び実施例）を参照して本願発明を説明したが、本願発明は上記実施形態（及び実施例）に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

この出願は、2009年3月24日に提出された日本出願特願2009-071217を基礎とする優先権を主張し、その開示の全てをここに取り込む。

【産業上の利用可能性】

【0010】

本発明は、トレーサビリティシステムに代表されるような、情報を複数のデータサーバ間で共有するシステムのアクセス制御、またはアクセス制御の自動化に適用できる。

【符号の説明】

【0011】

- 100 入出力装置
- 200 可搬型記憶装置
- 300 物流情報収集装置
- 400 物流情報アドレス解決装置
- 500 データサーバ
- 510 物流情報記憶部
- 520 通信部
- 530 証明付取得要求生成部
- 540 証明付取得要求処理部

10

20

30

40

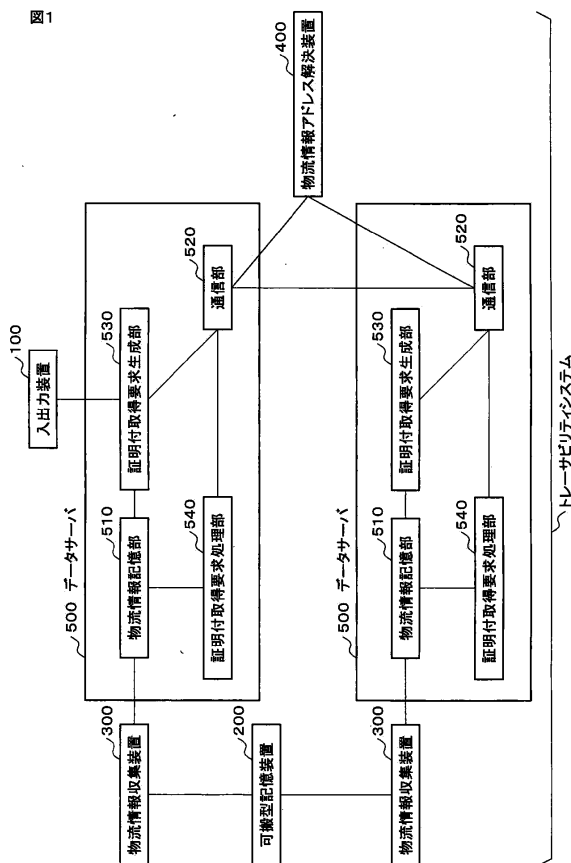
50

- 6 0 0 物流情報
- 6 2 0 固有識別子
- 6 3 0 イベント時刻
- 6 5 0 読み取り場所
- 6 6 0 タグの存在場所
- 6 7 0 センサデータ
- 6 7 1 計測開始時刻
- 6 7 2 計測終了時刻
- 6 7 3 計測間隔
- 6 7 4 計測値
- 6 7 5 非可逆要約情報
- 7 0 0 証明付取得要求
- 7 1 0 取得識別子
- 7 2 0 固有識別子
- 7 3 0 イベント時刻
- 7 5 0 場所
- 7 6 0 存在場所
- 7 7 0 センサデータ
- 7 7 1 計測開始時刻
- 7 7 2 計測終了時刻
- 7 7 3 計測間隔
- 7 7 4 計測値
- 7 7 5 非可逆要約情報
- 7 9 0 証明物流情報

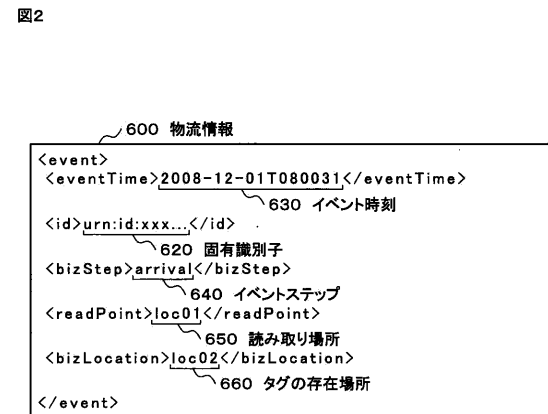
10

20

【図1】

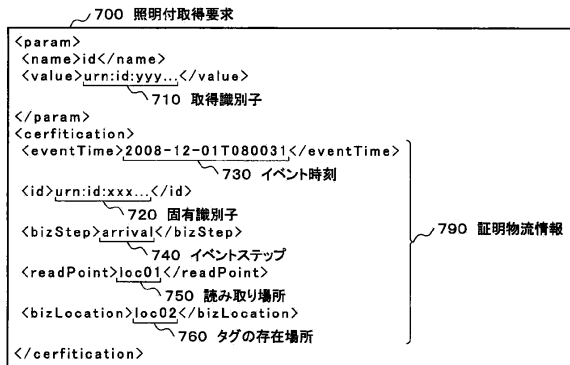


【図2】



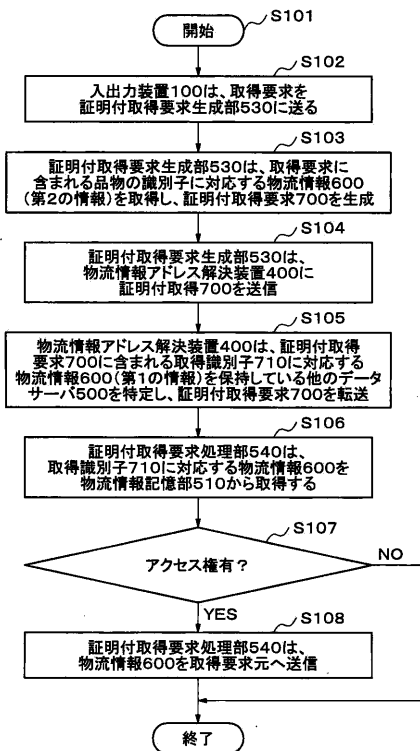
【図3】

図3



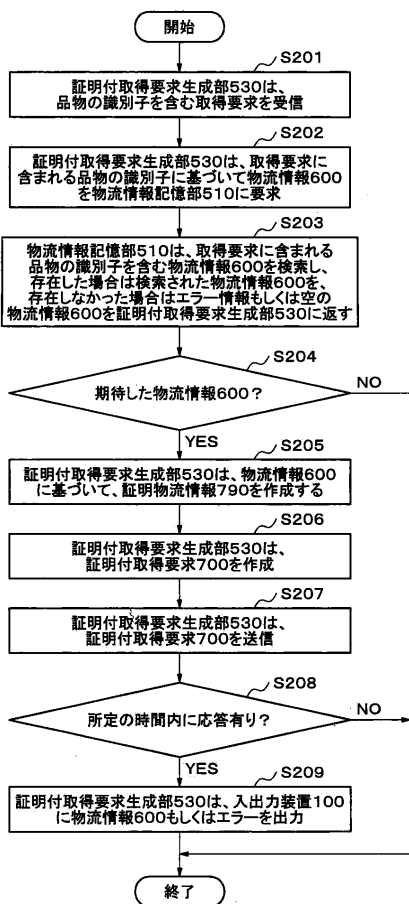
【図4】

図4



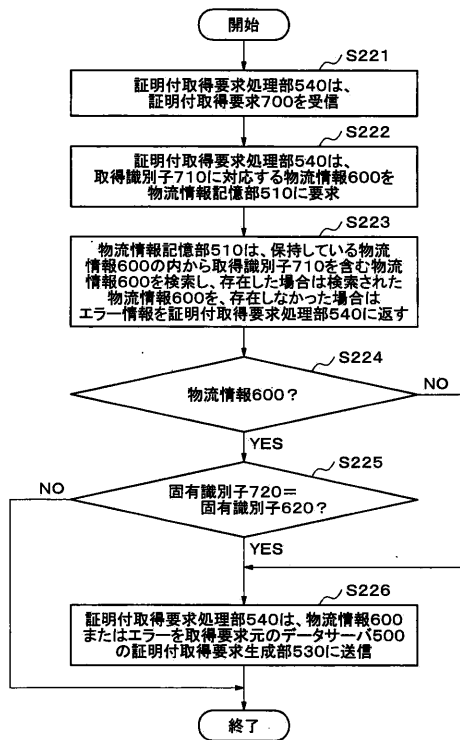
【図5】

図5



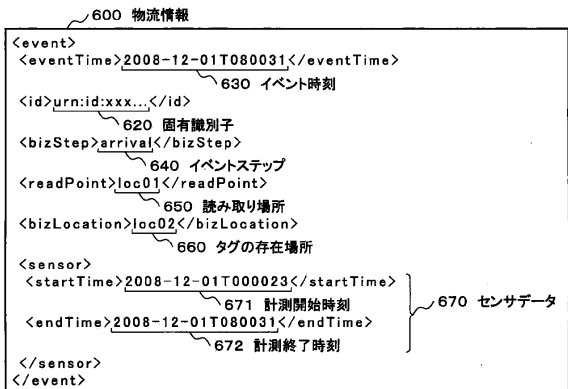
【図6】

図6



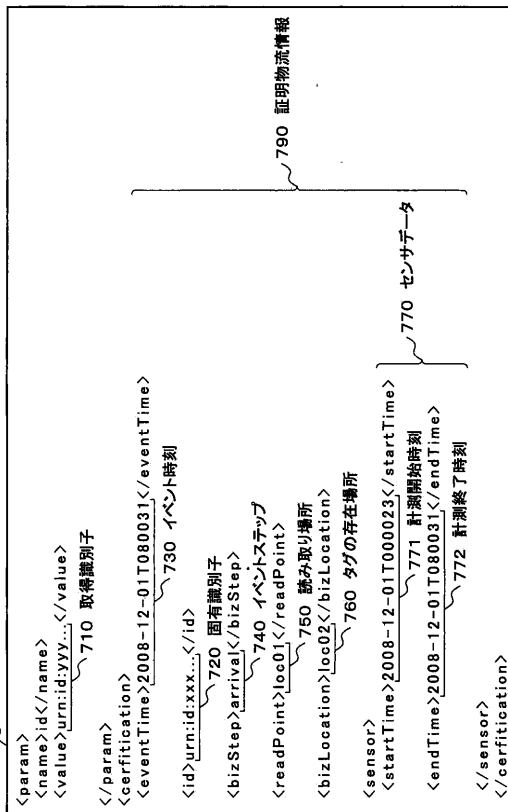
【 図 7 】

図7



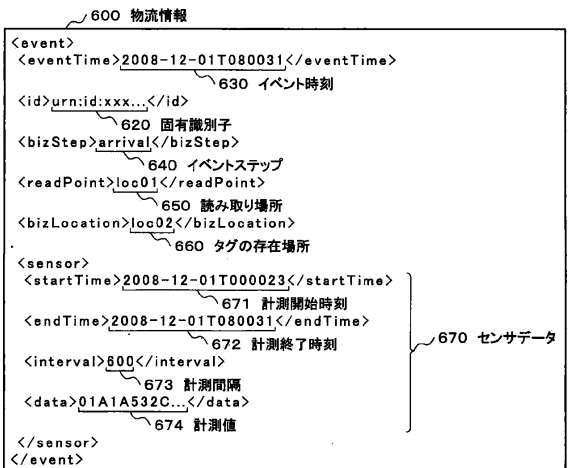
【 図 8 】

図8



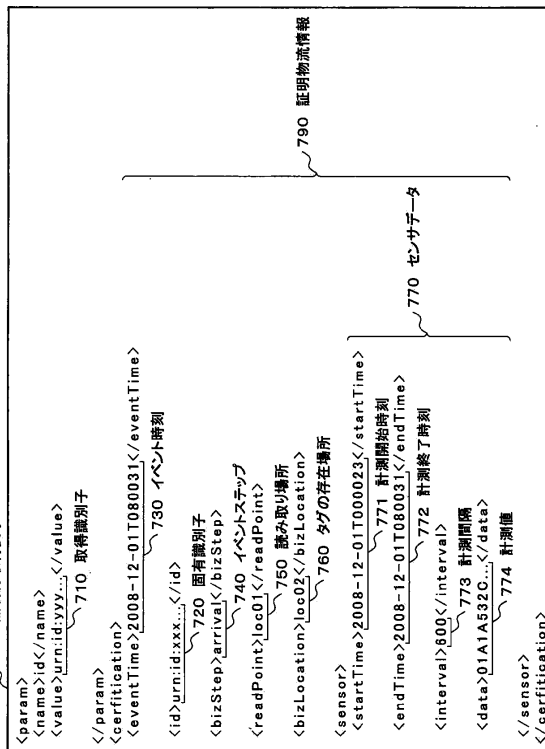
【 図 9 】

図9



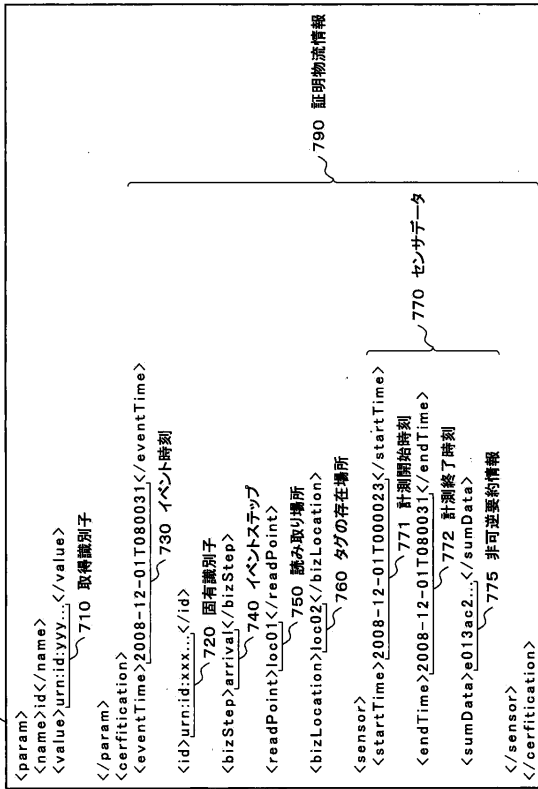
【 図 10 】

図10



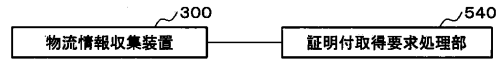
【 1 1 】

図11



【 1 2 】

図12



フロントページの続き

- (56)参考文献 特開2005-234628(JP,A)
特開2007-6144(JP,A)
特開2003-296515(JP,A)
特開2007-324945(JP,A)
特開2008-265940(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/60
G06Q 10/00
G06Q 50/00