

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-240596

(P2004-240596A)

(43) 公開日 平成16年8月26日(2004.8.26)

(51) Int.Cl.⁷

G06F 15/00

H04L 9/32

F I

G06F 15/00

H04L 9/00

330A

675B

テーマコード (参考)

5B085

5J104

審査請求 未請求 請求項の数 7 O L (全 9 頁)

(21) 出願番号 特願2003-27711 (P2003-27711)

(22) 出願日 平成15年2月5日(2003.2.5)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(74) 代理人 100093562

弁理士 児玉 俊英

(74) 代理人 100073759

弁理士 大岩 増雄

(74) 代理人 100088199

弁理士 竹中 孝生

(74) 代理人 100094916

弁理士 村上 啓吾

(72) 発明者 田中 慎也

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

最終頁に続く

(54) 【発明の名称】 Webシステム

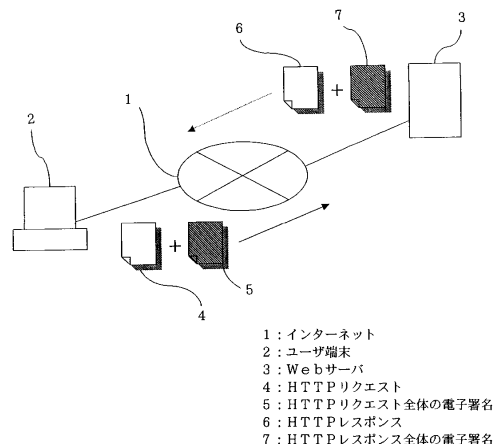
(57) 【要約】

【課題】電子フォームを含む電子データ全般について、否認及び改竄を防止できるWebシステムを得る。

【解決手段】ユーザ端末2は、Webサーバ3にWebページの送信要求を行うHTTPリクエスト4及びこのHTTPリクエストに対する電子署名5をインターネット1を介してWebサーバ3に送信し、Webサーバ3は、ユーザ端末2から送信されたHTTPリクエスト4によって要求されたWebページを含むHTTPレスポンス6及びこのHTTPレスポンスに対する電子署名7をインターネット1を介してユーザ端末2に送信するようして、ユーザ端末2の送信したHTTPリクエスト4が改竄なくWebサーバ3に届けられたことを確認し、Webサーバ3の送信したHTTPレスポンス6が改竄なくユーザ端末2に届けられたことを確認するようにした。

【選択図】

図1



【特許請求の範囲】

【請求項 1】

ネットワークを介して電子データを送受信する Web ブラウザを有するユーザ端末、及びこのユーザ端末との間で電子データを送受信する Web サーバを備え、上記ユーザ端末は、上記 Web サーバに電子データの送信要求を行う HTTP リクエスト及び上記 HTTP リクエストに対する電子署名を上記 Web サーバに送信するように構成され、上記 Web サーバは、上記 HTTP リクエストによって要求された電子データを含む HTTP レスポンス及び上記 HTTP レスポンスに対する電子署名を上記ユーザ端末に送信するように構成されていることを特徴とする Web システム。

【請求項 2】

10

上記ユーザ端末は、上記 HTTP レスポンス及び上記 HTTP レスポンスに対する電子署名を保存すると共に、上記 Web サーバは、上記 HTTP リクエスト及び上記 HTTP リクエストに対する電子署名を保存することを特徴とする請求項 1 記載の Web システム。

【請求項 3】

ネットワークを介して電子データを送受信する Web ブラウザを有するユーザ端末、このユーザ端末との間で電子データを送受信する Web サーバ、及び上記ユーザ端末と上記 Web サーバとの間の電子データの送受信に介在するように配置されたプロキシサーバを備え、上記ユーザ端末は、上記 Web サーバに電子データの送信要求を行う HTTP リクエストを上記プロキシサーバを介して上記 Web サーバに送信するように構成され、上記プロキシサーバは、上記ユーザ端末によって送信される HTTP リクエストに対する電子署名を生成して上記 HTTP リクエストと共に上記 Web サーバに送信するように構成され、上記 Web サーバは、上記 HTTP リクエストによって要求された電子データを含む HTTP レスポンス及び上記 HTTP レスポンスに対する電子署名を上記プロキシサーバに送信するように構成されていることを特徴とする Web システム。

20

【請求項 4】

上記プロキシサーバには、上記 HTTP リクエスト及び上記 HTTP リクエストに対する電子署名並びに上記 HTTP レスポンス及び上記 HTTP レスポンスに対する電子署名を保存する原本保存データベースを備えたことを特徴とする請求項 3 記載の Web システム。

【請求項 5】

30

上記ネットワークに接続され、時刻を計時するように構成されたタイムスタンプサーバを備え、上記タイムスタンプサーバの時刻は、上記原本保存データベースへの保存時に上記タイムスタンプサーバから取得され、上記取得された時刻が付加されて上記保存が行われることを特徴とする請求項 4 記載の Web システム。

【請求項 6】

上記ネットワークに接続され、時刻を計時するように構成されたタイムスタンプサーバを備え、上記タイムスタンプサーバの時刻は、上記電子署名の作成に際して上記タイムスタンプサーバから取得され、上記取得された時刻が上記電子署名に付加されることを特徴とする請求項 1～請求項 4 のいずれかに記載の Web システム。

【請求項 7】

40

上記ユーザ端末によって送信される HTTP リクエスト及び上記 Web サーバによって送信される HTTP レスポンスには、一連の送受信に対応したセッションを識別する識別子が付与されることを特徴とする請求項 1～請求項 6 のいずれかに記載の Web システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、通信ネットワークを介してユーザ端末と Web サーバとの間で電子データを送受信する Web システムに関するものである。

【0002】

【従来技術】

50

従来、通信ネットワークを介して電子フォームを送受信するシステムでは、送信する電子フォームに署名を付加することで改竄の防止を行っていた（例えば、特許文献1を参照）。

【0003】

【特許文献1】

特開2002-123632号公報（第3-7頁、第1図、第2図）

【0004】

【発明が解決しようとする課題】

従来の電子フォーム利用システムにおいては、電子署名をつける対象は、電子フォームであり、通常良く使用されるWebページ等のその他のデータは、対象とされていなかった。また、従来では、送信された電子フォームに対する改竄は、防止することができるが、送信者が送信したことを否認、受信者が受信したことを否認することに対する防止策はとられていなかった。 10

【0005】

この発明は、上記のような問題点を解決するためになされたものであり、電子フォームを含む電子データ全般について、否認及び改竄を防止できるWebシステムを得ることを目的とする。

【0006】

【課題を解決するための手段】

この発明に係わるWebシステムにおいては、ネットワークを介して電子データを送受信するWebブラウザを有するユーザ端末、及びこのユーザ端末との間で電子データを送受信するWebサーバを備え、ユーザ端末は、Webサーバに電子データの送信要求を行うHTTPリクエスト及びHTTPリクエストに対する電子署名をWebサーバに送信するように構成され、Webサーバは、HTTPリクエストによって要求された電子データを含むHTTPレスポンス及びHTTPレスポンスに対する電子署名をユーザ端末に送信するように構成されているものである。 20

【0007】

【発明の実施の形態】

実施の形態1.

以下、この発明の実施の形態1を図1に基づいて説明する。 30

図1は、この発明の実施の形態1によるWebシステムを示す概略構成図である。

図1において、ユーザ端末2は、インターネット1を介してWebサーバ3に接続されている。ユーザ端末2は、Webブラウザを用いて、Webサーバ3に、HTTPリクエスト4にHTTPリクエスト全体の電子署名5を付与して送信する。また、Webサーバ3は、ユーザ端末2に対して、HTTPレスポンス6にHTTPリクエスト全体の電子署名7を付与して送信する。

図2は、この発明の実施の形態1によるWebシステムの電子データのやりとりを示すフローチャートである。

【0008】

次に、動作を図2に基づいて説明する。 40

ユーザ端末2は、Webサーバ3に対して、Webページを要求し、Webサーバ3がその要求されたWebページを返す場合を想定する。

まず、ユーザ端末2は、送信するHTTPリクエスト全体の電子署名5を作成し、それをHTTPリクエスト4に付与してWebサーバ3に対して送信する（ステップ201）。Webサーバ3は、受信した電子署名5が正しいかどうか検証する（ステップ202）。ここで、ユーザ端末2の公開鍵証明書を検証するための証明書は、別途すでに入手済みであり、その証明書を用いて検証を行うものとする。

このように電子署名を検証することで、ユーザ端末2の送信したHTTPリクエスト4が改竄なく、Webサーバ3に届けられたということが確認できる。また、Webサーバ3がHTTPリクエスト4及び電子署名5を保存することで、HTTPリクエスト4を送信 50

したことに對してユーザ端末 2 が否認することを防止できる。

【0009】

電子署名 5 が正しい場合には、Webサーバ 3 は、HTTP リクエスト 4 に対する HTTP レスポンス 6 及びその HTTP レスポンス全体の電子署名 7 を作成し、ユーザ端末 2 に送信する（ステップ 203）。この HTTP レスポンス 6 には、ユーザ端末 2 から要求された Web ページが含まれる。ユーザ端末 2 は、受信した電子署名 7 が正しいかどうか検証する（ステップ 204）。ここで、Webサーバ 3 の公開鍵証明書を検証するための証明書は、別途すでに入手済みであり、その証明書を用いて検証を行うものとする。

このように、電子署名を検証することで、Webサーバ 3 の送信した HTTP レスポンス 6 が改竄なく、ユーザ端末 2 に届けられたということが確認できる。また、ユーザ端末 2 が HTTP レスポンス 6 及び電子署名 7 を保存しておくことで、HTTP レスポンス 6 を送信したことに對して、Webサーバ 3 が否認することを防止できる。

このような電子署名の機能は、Webサーバ、ブラウザが自動で電子署名を付与することで利用者がシームレスに利用することができる。

【0010】

実施の形態 1 によれば、ユーザ端末の送信した HTTP リクエストが改竄なく Webサーバに届けられたことを確認することができ、Webサーバが HTTP リクエスト及び電子署名を保存しておくことで、HTTP リクエストを送信したことに對してユーザ端末が否認することを防止できる。

また、Webサーバの送信した HTTP レスポンスが改竄なくユーザ端末に届けられたことを確認することができ、ユーザ端末が HTTP レスポンス及び電子署名を保存しておくことで、HTTP レスポンスを送信したことに對してWebサーバが否認することを防止できる。

さらに、このような電子署名の機能は、Webサーバ、ブラウザが自動で電子署名を付与することで利用者がシームレスに利用することができる。

【0011】

実施の形態 2.

図 3 は、この発明の実施の形態 2 による Web システムを電子フォームに適用した場合のフローチャートである。

図 4 は、この発明の実施の形態 2 による Web システムの電子フォーム表示例を示す図である。

図 4 において、電子フォーム 8 には、入力欄 9 と送信ボタン 10 が配置されている。

【0012】

実施の形態 1 では、1 回のメッセージのやり取りであったが、実施の形態 2 は、これをセッションという一連のメッセージのやり取りを認識する機構を適用した場合についてのものであり、電子フォームを例に挙げて説明する。

ここで電子フォームとは、例えば図 4 に示されるようなものである。ユーザ端末 2 において、図 4 の電子フォーム 8 中の入力欄 9 に必要事項を入力し、送信ボタン 10 を押下することで、入力データを Webサーバ 3 に送信し、その入力データを受け取った Webサーバ 3 が適切な処理を行うというように用いる。

このような電子フォームは、複数の電子フォームを経て、ある目的を達成するよう使用されることが多い。例えば、ショッピングカートを実現したシステムでは、ある電子フォームで商品 A を購入し、次の電子フォームで商品 B を購入、最後の電子フォームで会計処理を実行する、というように用いられる。

【0013】

電子フォームの場合の送受信の手順について、図 3 に従って説明する。

まず、ユーザ端末 2 は、Webサーバ 3 に対して、電子フォームを要求する（ステップ 301）。ここでステップ 301 では、特に電子署名を行わず、従来どおりの HTTP プロトコルで行う。Webサーバ 3 は、ユーザ端末 2 に対して、セッションを識別する識別子（以降セッション ID と呼ぶ）、及び要求された電子フォーム、さらに HTTP レスポ

10

20

30

40

50

ス全体の電子署名を返信する（ステップ302）。

次に、ユーザ端末2は、受信した電子署名が正しいかどうか検証した後で、電子フォームに必要事項を入力する（ステップ303）。続いて、送信ボタン10を押下することで、ユーザ端末2は、セッションID及び電子フォームの入力した内容を、HTTPプロトコルのPOSTリクエストでWebサーバ3に対して送信する。その際に、セッションID及び電子フォームに入力した内容を含むHTTPリクエスト全体の電子署名も付与する（ステップ304）。電子署名の付与は、Webブラウザが自動で行う。また、電子フォームに送信ボタンとは別の電子署名ボタンを用意し、それをユーザに押下させることで、電子署名を付与することもできる。

【0014】

Webサーバ3は、受信した電子署名が正しいかどうか検証する（ステップ305）。電子署名が正しい場合には、Webサーバ3は、電子フォームの受け付け処理を行い（ステップ306）、HTTPレスポンス及びそのHTTPレスポンス全体の電子署名を作成し、ユーザ端末2に送信する（ステップ307）。ここでHTTPレスポンスには、セッションID、及びWebサーバ3がユーザ端末2から送信された電子フォームを確かに受理したという旨のメッセージ、さらに次に電子フォームがある場合にはその電子フォームも含める。

次に、ユーザ端末2は、受信した電子署名が正しいかどうか検証する（ステップ308）。次の電子フォームが送信されている場合には、以上の手順と同様にその処理も行う。

【0015】

実施の形態2によれば、このような送受信の手順を実施することで、ユーザ端末2とWebサーバ3との間のやり取りを、改竄なく送信の否認を防止した形で行うことができる。また、これらのやり取りにセッションIDを含めることで、ユーザ端末2とWebサーバ3間のこれらのやり取りを一連のものとして管理することができる。

【0016】

実施の形態3.

図5は、この発明の実施の形態3によるWebシステムを示す概略構成図である。

図5において、1～7は図1におけるものと同一のものである。プロキシサーバ11は、ユーザ端末2とWebサーバ3間のやり取りに介在するように配置されている。

実施の形態1では、ユーザ端末2とWebサーバ3が直接HTTPプロトコルをやり取りしていたが、実施の形態3は、図5に示すように、ユーザ端末2とWebサーバ3の間にプロキシサーバ11を設けたものである。

【0017】

プロキシサーバ11が介在した場合の動作は、次のようになる。

まず、ユーザ端末2が送信したHTTPリクエストに対して、プロキシサーバ11は、電子署名を施し、Webサーバ3に転送を行う。さらに、Webサーバ3が送信したHTTPレスポンスとその電子署名の内、電子署名の部分を取り除いてユーザ端末2に転送する。

【0018】

実施の形態3によれば、以上のようにプロキシサーバを導入した場合には、複数のユーザ端末2の電子署名処理をプロキシサーバ11が代行して行うことができる。例えば、企業内に複数のユーザ端末2が存在する場合に、プロキシサーバ11がその企業の電子署名を施して、外部のWebサーバに送信することができるようになる。

【0019】

実施の形態4.

図6は、この発明の実施の形態4によるWebシステムを示す概略構成図である。

図6において、1～3、11は図5におけるものと同一のものである。プロキシサーバ11には原本保存データベース（DB）が設けられている。

実施の形態3では、ユーザ端末2とWebサーバ3の間にプロキシサーバ11を設け、そのプロキシサーバ11がユーザ端末2の行っていた電子署名を代行して行っていたが、実

10

20

30

40

50

施の形態 4 は、図 6 に示されるように、さらにプロキシサーバ 11 に原本保存 DB 12 を設けたものである。原本保存 DB 12 には、ユーザ端末 2 と Web サーバ 3 の間でやり取りされたデータを電子署名も含めて保存しておく。

【0020】

以上のようにすることで、例えば、プロキシサーバ 11 がある企業の署名を代行している場合、その企業と外部の Web サーバ 3 との間のやり取りの内容は、すべて原本保存 DB 12 に保存、一元管理することができる。その企業と外部の Web サーバ 3 との間のやり取りを閲覧したい場合には、プロキシサーバ 11 に閲覧したいデータを問い合わせればよい。

【0021】

実施の形態 4 によれば、ユーザ端末と Web サーバとのやり取りの内容を原本保存 DB により一元管理することができる。

【0022】

実施の形態 5.

図 7 は、この発明の実施の形態 5 による Web システムを示す概略構成図である。

図 7 において、1～3 は図 1 におけるものと同一のものである。タイムスタンプサーバ 13 は、ユーザ端末 2 と Web サーバ 3 間のやり取りにタイムスタンプを押すように配置されている。

実施の形態 1 では、ユーザ端末 2 と Web サーバ 3 が付与する電子署名内の署名時間には、ユーザ端末 2 と Web サーバ 3 自身の内部時計を用いていたが、実施の形態 5 は、図 7

に示すように、タイムスタンプサーバ 13 を用いたものである。
ユーザ端末 2 と Web サーバ 3 自身の内部時計を用いて署名を行う場合には、ユーザ自身による内部時計の改竄により実際に署名した時刻を偽ることができる。そこで、実施の形態 5 では、外部のタイムスタンプサーバ 13 を導入し、そこに信頼できる時刻を問い合わせ、返信された時刻を付与するようにユーザ端末 2、Web サーバ 3 に強要することで、上記問題を解決するようにした。

【0023】

また、実施の形態 4 において、プロキシサーバ 11 が原本保存 DB 12 に通信データ及び電子署名を保存する際にも、タイムスタンプサーバ 13 を利用することができる。これによりプロキシサーバ 11 が原本保存 DB 12 に保存した時間が信頼できるものになり、保存した原本が、より信頼できるものになる。

【0024】

実施の形態 5 によれば、ユーザ端末と Web サーバが、自身の内部時計を用いて署名を行う場合に、ユーザ自身による内部時計の改竄により実際に署名した時刻を偽るといったことを防止することができる。

また、プロキシサーバが原本保存 DB に保存する時間を信頼できるものにすることができ、保存した原本が、より信頼できるものになる。

【0025】

【発明の効果】

この発明は、以上説明したように構成されているので、以下に示すような効果を奏する。
ネットワークを介して電子データを送受信する Web ブラウザを有するユーザ端末、及びこのユーザ端末との間で電子データを送受信する Web サーバを備え、ユーザ端末は、Web サーバに電子データの送信要求を行う HTTP リクエスト及び HTTP リクエストに対する電子署名を Web サーバに送信するように構成され、Web サーバは、HTTP リクエストによって要求された電子データを含む HTTP レスポンス及び HTTP レスポンスに対する電子署名をユーザ端末に送信するように構成されているので、ユーザ端末の送信した HTTP リクエストが改竄なく Web サーバに届けられたことを確認することができる、Web サーバの送信した HTTP レスポンスが改竄なくユーザ端末に届けられたことを確認することができる。

【図面の簡単な説明】

10

20

30

40

50

【図 1】 この発明の実施の形態 1 による W e b システムを示す概略構成図である。

【図 2】 この発明の実施の形態 1 による W e b システムの電子データのやりとりを示すフローチャートである。

【図 3】 この発明の実施の形態 2 による W e b システムを電子フォームに適用した場合のフローチャートである。

【図 4】 この発明の実施の形態 2 による W e b システムの電子フォーム表示例を示す図である。

【図 5】 この発明の実施の形態 3 による W e b システムを示す概略構成図である。

【図 6】 この発明の実施の形態 4 による W e b システムを示す概略構成図である。

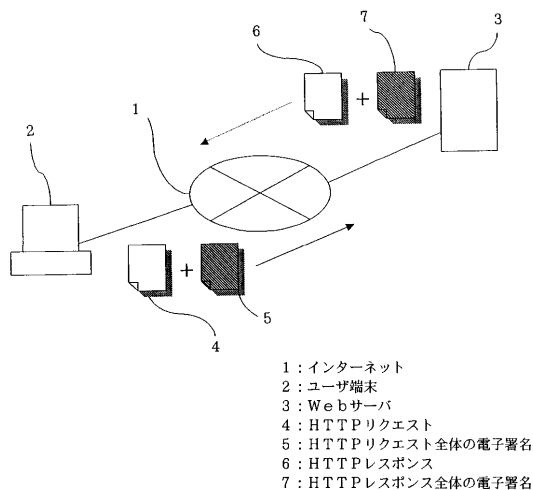
【図 7】 この発明の実施の形態 5 による W e b システムを示す概略構成図である。

10

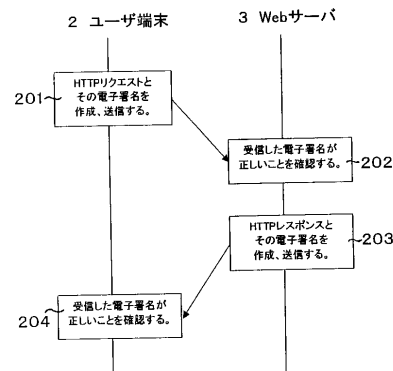
【符号の説明】

- 1 インターネット、2 ユーザ端末、3 W e b サーバ、
 4 H T T P リクエスト、5 H T T P リクエスト全体の電子署名、
 6 H T T P レスポンス、7 H T T P レスポンス全体の電子署名、
 8 電子フォーム、9 入力欄、10 送信ボタン、11 プロキシサーバ、
 12 原本保存 D B、13 タイムスタンプサーバ。

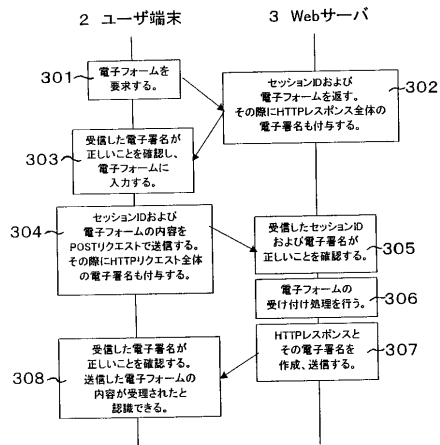
【図 1】



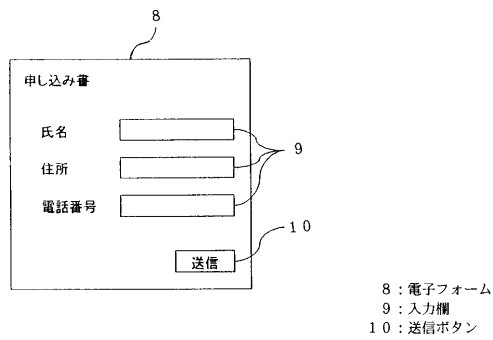
【図 2】



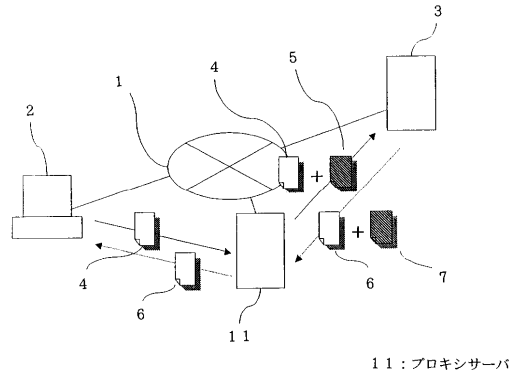
【図 3】



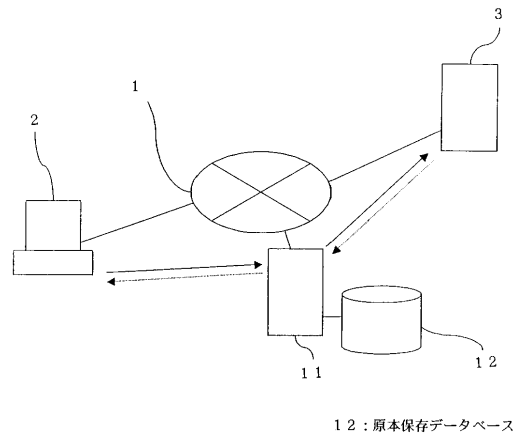
【図 4】



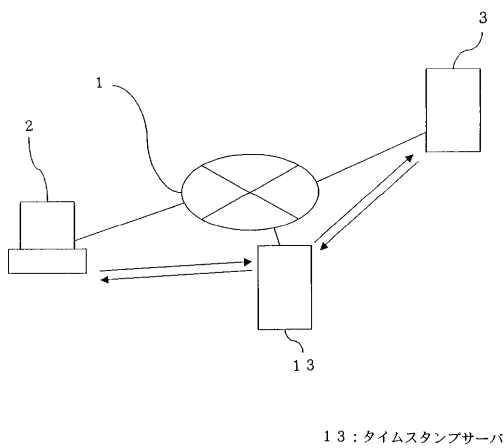
【図 5】



【図 6】



【図 7】



フロントページの続き

- (72)発明者 野村 立
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 長谷川 伸
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 森本 和成
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- Fターム(参考) 5B085 AA08 AE00 AE23 BG02 BG07
5J104 AA09 PA08 PA09