(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2014-167672
(P2014-167672A)
(43)公開日　平成26年9月11日(2014.9.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/20	131D	5J104
H04L 9/32	(2006.01)	H04L	9/00	675B	
G06F 21/62	(2013.01)	G06F	21/24	166A	

審査請求 未請求　請求項の数 8　ＯＬ　（全 25 頁）

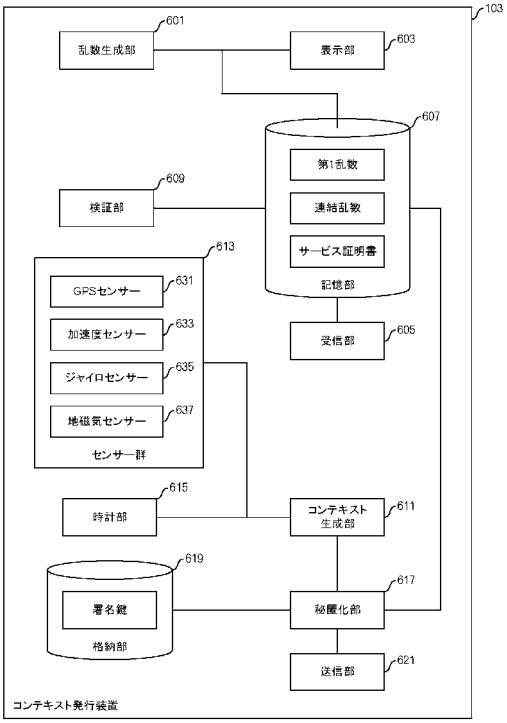
(21)出願番号　特願2013-38616(P2013-38616)
(22)出願日　平成25年2月28日(2013.2.28)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100103528
弁理士　原田　一男
(72)発明者　大久保　隆夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考)　5J104 AA07 AA16 AA32 EA04 EA19 JA21 KA02 KA05 NA37 NA38 PA07

(54)【発明の名称】情報処理装置、認証システム及びプログラム

(57)【要約】　（修正有）
【課題】コンテキストに基づくネットワーク認証に係る不正行為を防止する。
【解決手段】情報処理装置は、コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、コンテキストを生成する第１の生成部と、コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、署名データと被署名データとを送信する送信部とを有する。被認証装置から要求を受けた情報処理装置側でコンテキストを生成し、更に署名を付することで、被認証装置における不正なコンテキストの生成やコンテキストの改変を防止する。
【選択図】図６



【特許請求の範囲】
【請求項１】
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成する第１の生成部と、
前記コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、
前記署名データと前記被署名データとを送信する送信部と
を有する情報処理装置。
【請求項２】
更に、
前記認証装置において前記被認証装置を検証するための情報と前記コンテキストとを含む前記被署名データを生成する第３の生成部
を有する請求項１記載の情報処理装置。
【請求項３】
前記送信部は、前記署名データと前記被署名データとを、前記認証装置へ送信する
請求項１又は２記載の情報処理装置。
【請求項４】
更に、
不規則に生成されたデータを表示する表示部と、
前記不規則に生成されたデータを受信することにより、当該データの送信元である前記被認証装置を検証する第１の検証部と
を有する請求項１乃至３のいずれか１つ記載の情報処理装置。
【請求項５】
更に、
前記認証装置の公開鍵により、少なくとも前記被署名データを暗号化する暗号化部
を有する請求項１乃至４のいずれか１つ記載の情報処理装置。
【請求項６】
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成する第１の生成部と、
前記コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、
前記署名データと前記被署名データとを送信する送信部と
を有する情報処理装置と、
前記署名データと前記被署名データとを受信すると、前記署名データに基づく検証を行う第１の検証部と、
前記被署名データに含まれる前記コンテキストに対する検証を行う第２の検証部と
を有する認証装置と
を含む認証システム。
【請求項７】
前記認証装置は、更に、
前記被署名データに含まれるコンテキスト固有のデータに基づいて、前記コンテキストの再利用を検出する検出部
を有する請求項８記載の認証システム。
【請求項８】
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成し、
前記コンテキストを含む被署名データに対する署名データを生成し、
前記署名データと前記被署名データとを送信する
処理をコンピュータ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】

本技術は、ネットワーク認証技術に関する。
【背景技術】
【０００２】
ネットワーク認証の多くは、ユーザ情報を根拠としている。ある特許文献には、シングルサインオンを提供するケルベロス(Kerberos)認証を前提として、ユーザの信頼度に応じてアクセス可能なサービスを制限する技術が開示されている。
【０００３】
しかし、ユーザＩＤやパスワードのようなユーザ情報が流出した場合には、他人によるなりすましが行われる恐れがある。
【０００４】
一方、装置の位置情報を根拠として認証を行う技術もある。別の特許文献では、電子名刺のような電子データを携帯装置間で安全に交換するために、相手装置の位置情報と自装置の位置情報の関係に基づいて相互認証を行っている。
【０００５】
このように装置の位置情報を根拠とする場合、被認証装置は、例えばその装置自身が備えるＧＰＳ（Global Positioning System）センサーで測定した位置情報に基づくコンテキストを認証装置に送る。そして、認証装置は、被認証装置から送られるコンテキストが真正であることを前提として、ネットワーク認証を行うことになる。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００３－２３３５８６号公報
【特許文献２】特開２００６－１５７６３５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
本技術の目的は、一側面では、コンテキストに基づくネットワーク認証に係る不正行為を防止することを目的とする。
【課題を解決するための手段】
【０００８】
一態様に係る情報処理装置は、コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、コンテキストを生成する第１の生成部と、コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、署名データと被署名データとを送信する送信部とを有する。
【発明の効果】
【０００９】
一側面としては、コンテキスに基づくネットワーク認証に係る不正行為を防止することができる。
【図面の簡単な説明】
【００１０】
【図１】図１は、コンテキスト依存サービスに係るシステム構成例を示す図である。
【図２】図２は、コンテキスト依存サービスの利用態様の例を示す図である。
【図３】図３は、コンテキスト依存サービスの利用態様の例を示す図である。
【図４】図４は、コンテキスト依存サービスの利用態様の例を示す図である。
【図５】図５は、装置間のデータフローの例を示す図である。
【図６】図６は、コンテキスト発行装置のモジュール構成例を示す図である。
【図７】図７は、利用者端末のモジュール構成例を示す図である。
【図８】図８は、コンテキスト依存サーバのモジュール構成例を示す図である。
【図９】図９は、シーケンス例を示す図である。
【図１０】図１０は、シーケンス例を示す図である。

【図１１】図１１は、秘匿化部の内部構成の例を示す図である。
【図１２】図１２は、シーケンス例を示す図である。
【図１３】図１３は、検証部の内部構成の例を示す図である。
【図１４】図１４は、シーケンス例を示す図である。
【図１５】図１５は、実施の形態２に係る装置間のデータフローの例を示す図である。
【図１６】図１６は、実施の形態２に係るコンテキスト発行装置のモジュール構成例を示す図である。
【図１７】図１７は、実施の形態２に係る利用者端末のモジュール構成例を示す図である。
【図１８】図１８は、実施の形態２に係るシーケンス例を示す図である。
【図１９】図１９は、実施の形態２に係るシーケンス例を示す図である。
【図２０】図２０は、実施の形態２に係るシーケンス例を示す図である。
【図２１】図２１は、実施の形態２に係るシーケンス例を示す図である。
【図２２】図２２は、コンテキスト発行装置のハードウエア構成例を示す図である。
【図２３】図２３は、コンテキスト依存サーバのハードウエア構成例を示す図である。
【発明を実施するための形態】
【００１１】
［実施の形態１］
コンテキスト依存サービスでは、利用者が保持する装置（本実施の形態では、利用者の近くにある装置）が備えるセンサーで測定したセンサーデータ（例えば、位置データや時間データ）に基づくコンテキストを利用して、サービスへのアクセスを制限する。
【００１２】
本実施の形態は、コンテキスト依存サービスにおける不正利用を排除する。想定される脅威には、例えば、センサーデータの改竄による不正なコンテキストの生成、コンテキストの不正な改変、コンテキストの不正な流用や転用などがある。
【００１３】
また、利用者自身が不正に関与することも考えられる。利用者装置内のセンサーで計測されたセンサーデータは、利用者が改竄しやすい状況にある。また、利用者装置がマルウエアに感染している場合には、コンテキストが流出する可能性もある。
【００１４】
本実施の形態では、利用者装置の他に、コンテキストを発行する装置を設ける。
【００１５】
図１に、コンテキスト依存サービスに係るシステム構成例を示す。利用者端末１０１は、インターネットに接続可能であり、利用者が保持する装置である利用者端末１０１として、例えば携帯電話端末、タブレット端末、あるいはパーソナルコンピューターなどが用いられる。
【００１６】
コンテキスト発行装置１０３は、コンテキストを発行する装置である。コンテキスト発行装置１０３は、インターネットに接続可能である。コンテキスト発行装置１０３の信頼性が高ければ、前述の脅威は軽減される。例えば、耐タンパー性に優れ、マルウエアに感染しないように管理されていれば、コンテキスト発行装置１０３の信頼性は高い。
【００１７】
コンテキストは、時間や位置等のデータを含む。あるいは、時間や位置の条件に基づいて分類された識別子であってもよい。
【００１８】
コンテキスト依存サーバ１０５（図１では１０５ａ乃至１０５ｃ）は、コンテキストに基づく認証を行う。つまり、コンテキスト依存サーバ１０５は、認証装置の例である。また、この例で、コンテキスト依存サーバ１０５は、サービスの提供も行う。但し、コンテキストに基づく認証を行う装置と、サービスを提供する装置とは、別に設けてもよい。
【００１９】

続いて、図２乃至４を用いて、コンテキスト依存サービスの利用態様について説明する。図２は、利用者がコンテキスト発行装置１０３を保持し、複数の利用者端末１０１の各々からコンテキスト依存サービスを利用する形態を示している。

【００２０】

時刻Ｔ１において、利用者は訪問先２０１でコンテキスト依存サービスを利用する。このとき、利用者は、携帯型の利用者端末１０１ａをコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ１が訪問予定時間帯に含まれ、位置が訪問先２０１を指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１ａはコンテキスト依存サーバ１０５で管理する営業データにアクセスする。

【００２１】

続いて、時刻Ｔ２において、利用者は会社２０３でコンテキスト依存サービスを利用する。このとき、利用者は、デスクトップ型の利用者端末１０１ｂをコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ２が就業時間帯に含まれ、位置が会社２０３内を指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１ｂはコンテキスト依存サーバ１０５で管理する社内ＤＢにアクセスする。

【００２２】

更に、時刻Ｔ３において、利用者は自宅２０５でコンテキスト依存サービスを利用する。このとき、利用者は、ノート型の利用者端末１０１ｃをコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ３が自宅勤務の時間帯に含まれ、位置が自宅２０５を指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１ｃはコンテキスト依存サーバ１０５で管理する掲示板にアクセスする。

【００２３】

図３は、利用者以外の者が保持するコンテキスト発行装置１０３とペアリングして利用者端末１０１からコンテキスト依存サービスを利用する形態を示している。

【００２４】

この例は、複数の施設を見学する場合を想定している。引率者が、コンテキスト発行装置１０３を携帯している。見学する利用者は、携帯型の利用者端末１０１を保持している。

【００２５】

時刻Ｔ４において、利用者は施設３０１ａでコンテキスト依存サービスを利用する。利用者は、利用者端末１０１を引率者が保持するコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ４が施設３０１ａの見学予定時間帯に含まれ、位置が施設３０１ａを指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１はコンテキスト依存サーバ１０５から施設３０１ａについてのガイダンスをダウンロードする。

【００２６】

続いて、時刻Ｔ５において、利用者は施設３０１ｂでコンテキスト依存サービスを利用する。利用者は、利用者端末１０１を引率者が保持するコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ５が施設３０１ｂの見学予定時間帯に含まれ、位置が施設３０１ｂを指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１はコンテキスト依存サーバ１０５から施設３０１ｂについてのガイダンスをダウンロードする。

【００２７】

更に、時刻Ｔ６において、利用者は施設３０１ｃでコンテキスト依存サービスを利用する。利用者は、利用者端末１０１を引率者が保持するコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻Ｔ６が施設３０１ｃの見学予定時間帯に含まれ、位置が施設３０１ｃを指している場合に認

証成功と判断する。認証に成功すると、利用者端末１０１はコンテキスト依存サーバ１０５から施設３０１ｃについてのガイダンスをダウンロードする。

【００２８】

図５は、特定場所に設置されたコンテキスト発行装置１０３とペアリングして任意の利用者端末１０１からコンテキスト依存サービスを利用する形態を示している。

【００２９】

この例は、展示会に不特定の参加者が訪れる場合を想定している。コンテキスト発行装置１０３は、展示会の会場に設置されている。展示会に参加する利用者の各々は、それぞれ携帯型の利用者端末１０１ｄ乃至ｆを保持している。

【００３０】

展示会の会場で、各利用者は、時刻Ｔ７からＴ８までの間に、自らの利用者端末１０１を展示会の会場４０１に設置されているコンテキスト発行装置１０３とペアリングさせる。コンテキスト依存サーバ１０５は、コンテキストにより特定される時刻が展示会の開催時間帯に含まれ、位置が会場４０１を指している場合に認証成功と判断する。認証に成功すると、利用者端末１０１ｄ乃至ｆはコンテキスト依存サーバ１０５で提供する展示物紹介のＷｅｂページを表示する。

【００３１】

続いて、本実施の形態に係る動作の概要について説明する。図５に、装置間のデータフローの例を示す。コンテキスト発行装置１０３は、コンテキスト発行装置１０３で生成した第１乱数を表示する（Ｓ５０１）。利用者は、第１乱数を目視し、利用者端末１０１に第１乱数を入力する。第１乱数は、コンテキスト発行装置１０３に送られ、コンテキスト発行装置１０３で第１乱数を検証することによって、利用者端末１０１とコンテキスト発行装置１０３との間のペアリングが行われる。つまり、第１乱数は、利用者端末１０１がコンテキスト発行装置１０３の近くから操作されていることを担保するために用いられる。

【００３２】

利用者端末１０１は、コンテキスト依存サーバ１０５へコンテキスト依存サーバ１０５の証明書（以下、サービス証明書という。）を要求する（Ｓ５０３）。コンテキスト依存サーバ１０５は、利用者端末１０１からの要求に応じて、サービス証明書を利用者端末１０１に返信する（Ｓ５０５）。サービス証明書の検証によって、コンテキスト依存サーバ１０５が正当であることが担保される。

【００３３】

利用者端末１０１は、コンテキスト発行装置１０３へコンテキストの発行を依頼する（Ｓ５０７）。コンテキスト発行依頼のデータには、前述の第１乱数が含まれている。

【００３４】

コンテキスト発行装置１０３は、種々の検証を行った上で、コンテキストを生成し、更に生成したコンテキストを秘匿化し、秘匿化コンテキストデータ（以下、秘匿化コンテキスト）を利用者端末１０１に返信する（Ｓ５０９）。

【００３５】

利用者端末１０１は、コンテキスト依存サーバ１０５にアクセスを要求する（Ｓ５１１）。アクセス要求のデータには、前述の秘匿化コンテキストが含まれている。

【００３６】

コンテキスト依存サーバ１０５は、秘匿化コンテキストに対して種々の検証を行う。そして、コンテキストが所定の条件を満たす場合に、認証成功と判定し、利用者端末１０１に対してアクセスチケットを返信する（Ｓ５１３）。

【００３７】

利用者端末１０１は、アクセスチケットを取得すると、そのアクセスチケットを送ることによって（Ｓ５１５）、コンテキスト依存サーバ１０５で提供するサービスを受ける（Ｓ５１７）。アクセスチケットを発したコンテキスト依存サーバ１０５以外のコンテキスト依存サーバ１０５で、サービスを提供するようにしてもよい。

【００３８】
続いて、各装置のモジュール構成について説明する。まず、コンテキスト発行装置１０３のモジュール構成について説明する。図６に、コンテキスト発行装置１０３のモジュール構成例を示す。コンテキスト発行装置１０３は、乱数生成部６０１、表示部６０３、受信部６０５、記憶部６０７、検証部６０９、コンテキスト生成部６１１、センサー群６１３、時計部６１５、秘匿化部６１７、格納部６１９及び送信部６２１を有している。
【００３９】
乱数生成部６０１は、第１乱数を生成する。表示部６０３は、第１乱数を表示する。受信部６０５は、インターネットを介してデータを受信する。
【００４０】
記憶部６０７は、種々のデータを記憶する。この例では、第１乱数、コンテキスト発行依頼のデータに含まれる連結乱数とサービス証明書を記憶している。連結乱数は、第１乱数と、利用者端末１０１で生成した第２乱数とを連結したデータである。
【００４１】
検証部６０９は、コンテキスト発行依頼のデータについて、種々の検証を行う。コンテキスト生成部６１１は、センサーデータや時刻などに基づいて、コンテキストデータを生成する。
【００４２】
センサー群６１３は、種々のセンサーを含んでいる。この例で、センサー群６１３は、ＧＰＳセンサー６３１、加速度センサー６３３、ジャイロセンサー６３５及び地磁気センサー６３７を含んでいる。ＧＰＳセンサー６３１は、位置データを計測する。加速度センサー６３３は、加速度を計測する。ジャイロセンサー６３５は、角度や角速度を計測する。地磁気センサー６３７は、地磁気の向きを検知する。地磁気センサー６３７は、更に地磁気の向きに基づき、方位を計測する。センサー群６１３は、他のセンサーを含むようにしてもよい。時計部６１５は、日付と時刻とを計測する。
【００４３】
秘匿化部６１７は、コンテキストを秘匿化する。格納部６１９は、コンテキスト発行装置１０３の署名鍵などのデータを格納している。送信部６２１は、インターネットを介してデータを送信する。
【００４４】
次に、利用者端末１０１のモジュール構成について説明する。図７に、利用者端末１０１のモジュール構成例を示す。利用者端末１０１は、受信部７０１、送信部７０３、受付部７０５、サービス証明書取得部７０７、記憶部７０９、検証部７１１、乱数生成部７１３、コンテキスト発行依頼部７１５、アクセスチケット取得部７１７及びサービス取得部７１９を有している。
【００４５】
受信部７０１は、インターネットを介してデータを受信する。送信部７０３は、インターネットを介してデータを送信する。受付部７０５は、第１乱数の入力を受け付ける。サービス証明書取得部７０７は、コンテキスト依存サーバ１０５からサービス証明書を取得する。
【００４６】
記憶部７０９は、種々のデータを記憶する。この例で、記憶部７０９は、第１乱数、サービス証明書、コンテキスト条件及び連結乱数を記憶する。
【００４７】
検証部７１１は、種々の検証を行う。乱数生成部７１３は、第１乱数と第２乱数とを連結させた連結乱数を生成する。コンテキスト発行依頼部７１５は、コンテキスト発行装置１０３にコンテキストの発行を依頼し、秘匿化コンテキストを取得する。アクセスチケット取得部７１７は、コンテキスト依存サーバ１０５に秘匿化コンテキストを転送し、アクセスチケットを取得する。サービス取得部７１９は、コンテキスト依存サーバ１０５にアクセスチケットを送り、コンテキスト依存サーバ１０５により提供されるサービスを受け

る。
【００４８】
次に、コンテキスト依存サーバ１０５のモジュール構成について説明する。図８に、コンテキスト依存サーバ１０５のモジュール構成例を示す。コンテキスト依存サーバ１０５は、受信部８０１、送信部８０３、サービス証明書発行部８０５、格納部８０７、アクセスチケット発行部８０９、記憶部８１１、検証部８１３、登録部８１５、ハッシュ値ＤＢ８１７、サービス提供部８１９及び判定部８２１を有している。
【００４９】
受信部８０１は、インターネットを介してデータを受信する。送信部８０３は、インターネットを介してデータを送信する。
【００５０】
格納部８０７は、種々のデータを格納している。この例で、格納部８０７は、サービス証明書、コンテキスト条件、秘密鍵及びアクセスチケットを格納している。コンテキスト条件は、コンテキストの検証に用いられる。秘密鍵は、コンテキスト依存サーバ１０５固有の秘密鍵である。
【００５１】
アクセスチケット発行部８０９は、アクセス要求に応じて、アクセスチケットを発行する。記憶部８１１は、種々のデータを記憶する。この例で、記憶部８１１は、暗号化署名データ、暗号化被署名データ及び連結乱数を記憶する。
【００５２】
検証部８１３は、種々の検証を行う。登録部８１５は、秘匿化コンテキストから抽出されたハッシュ値をハッシュ値ＤＢ８１７に登録する。ハッシュ値ＤＢ８１７は、既に利用されたコンテキストを識別するためのハッシュ値を記憶する。ハッシュ値は、コンテキスト固有のデータの例である。サービス提供部８１９は、アクセスチケットに応じて、サービスを提供する。判定部８２１は、アクセスチケットの正当性を判定する。
【００５３】
図９、図１０、図１２及び図１４に示したシーケンスに沿って、各装置の動作について説明する。まず、図９に示したシーケンスについて説明する。
【００５４】
コンテキスト発行装置１０３側で、乱数生成部６０１は、第１乱数を生成する（Ｓ９０１）。表示部６０３は、生成した第１乱数を表示する（Ｓ９０３）。利用者は、第１乱数を目視で確認し、利用者端末１０１に入力する（Ｓ９０５）。
【００５５】
利用者端末１０１側で、受付部７０５は、第１乱数入力を受け付ける（Ｓ９０７）。
【００５６】
更に、利用者端末１０１側で、サービス証明書取得部７０７は、コンテキスト依存サーバ１０５からコンテキスト条件とサービス証明書とを取得する（Ｓ９０９）。このとき、サービス証明書取得部７０７は、送信部７０３から証明書要求のデータをコンテキスト依存サーバ１０５に送信する（Ｓ９１１）。
【００５７】
コンテキスト依存サーバ１０５側で、受信部８０１が証明書要求のデータを受信すると、サービス証明書発行部８０５は、格納部８０７からサービス証明書とコンテキスト条件とを読み出して、送信部８０３を介して利用者端末１０１に返信する（Ｓ９１３）。
【００５８】
コンテキスト条件は、利用者端末１０１側の予備的な検証に用いられる。従って、利用者端末１０１側で予備的な検証を行わない場合には、コンテキスト条件を送信しないようにしてもよい。
【００５９】
利用者端末１０１側で、受信部７０１でサービス証明書とコンテキスト条件とを受信すると、サービス証明書取得部７０７は、サービス証明書とコンテキスト条件とを記憶部７

０９に記憶させる。尚、コンテキスト条件を受信しない場合には、コンテキスト条件は記憶させない。

【００６０】

更に、利用者端末１０１側で、検証部７１１は、コンテキスト条件を検証する（Ｓ９１５）。この検証は、コンテキスト条件を満たさないことが自明の場合に処理を中断するための予備的な検証である。検証部７１１は、サービス証明書を検証する（Ｓ９１７）。この検証も、不正なコンテキスト依存サーバ１０５であることを予め検出するための予備的処理である。従って、Ｓ９１５とＳ９１７との検証は、省略されるようにしてもよい。

【００６１】

更に、利用者端末１０１側で、乱数生成部７１３は、第２乱数を生成する（Ｓ９１９）。更に、乱数生成部７１３は、記憶部７０９に記憶させている第１乱数と、第２乱数とを連結する（Ｓ９２１）。生成した連結乱数は、記憶部７０９に記憶される。このとき、生成した第２乱数を表示し、利用者に第２乱数を入力させるようにしてもよい。

【００６２】

更に、利用者端末１０１側で、コンテキスト発行依頼部７１５は、コンテキスト条件に基づいてコンテキスト発行装置１０３を選択する（Ｓ９２３）。例えば、コンテキスト条件で判定する情報を測定可能なコンテキスト発行装置１０３が選択される。但し、当該選択処理は省いてもよい。

【００６３】

更に、利用者端末１０１側で、コンテキスト発行依頼部７１５は、コンテキスト発行装置１０３にコンテキスト発行を依頼する（Ｓ９２５）。このとき、コンテキスト発行依頼部７１５は、送信部７０３からコンテキス発行依頼のデータをコンテキスト発行装置１０３に送信する（Ｓ９２７）。コンテキス発行依頼のデータには、連結乱数とサービス証明書とが含まれている。

【００６４】

コンテキスト発行装置１０３側で、受信部６０５は、コンテキス発行依頼のデータを受信すると、連結乱数とサービス証明書とを記憶部６０７に記憶させる。

【００６５】

図１０に、シーケンスの続きを示す。コンテキスト発行装置１０３側で、検証部６０９は、第１乱数を検証する（Ｓ１００１）。具体的には、検証部６０９は、連結乱数から第１乱数を抽出する。抽出した第１乱数が、記憶部６０７に記憶されている第１乱数と一致するか否かを判定する。抽出した第１乱数が、記憶部６０７に記憶されている第１乱数と一致すると判定した場合には、検証成功と判断し、処理を続行する。抽出した第１乱数が、記憶部６０７に記憶されている第１乱数と一致しないと判定した場合には検証失敗と判断し、第１乱数の検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。この例で、第１乱数の検証成功は、ペアリングが成立したことを意味する。

【００６６】

続いて、コンテキスト発行装置１０３側で、検証部６０９は、サービス証明書を検証する（Ｓ１００３）。証明書の検証方法は、従来の技術に従う。サービス証明書の検証に成功した場合には、処理を続行する。サービス証明書の検証に失敗した場合には、サービス証明書の検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。

【００６７】

更に、コンテキスト発行装置１０３側のＳ１００５乃至Ｓ１００９の処理でコンテキストが生成される。コンテキスト生成部６１１は、センサー群６１３からセンサーデータを取得する（Ｓ１００５）。センサー群６１３のうち、一部のセンサーデータを取得するようにしてもよい。コンテキスト生成部６１１は、更に、時計部６１５から現在時刻を取得する（Ｓ１００７）。コンテキスト生成部６１１は、現在時刻に併せて当日の日付も取得するようにしてもよい。コンテキスト生成部６１１は、コンテキストデータを生成する（Ｓ１００９）。この例で、コンテキストデータは、センサーデータや現在時刻を含む。但し、コンテキスト生成部６１１は、センサーデータや現在時刻に基づいて分類された状況

や状態に関する識別子を生成し、当該識別子をコンテキストデータに含めるようにしてもよい。

【００６８】

続いて、秘匿化部６１７は、Ｓ１０１１乃至Ｓ１０１７の処理で、コンテキストを秘匿化する。

【００６９】

図１１に、秘匿化部６１７の内部構成の例を示す。秘匿化部６１７は、算出部１１０１、被署名データ生成部１１０３、署名生成部１１０５、抽出部１１０７及び暗号化部１１０９を有している。算出部１１０１は、ハッシュ値の算出処理を行う。被署名データ生成部１１０３は、被署名データを生成する。署名生成部１１０５は、電子署名を生成する処理を行う。抽出部１１０７は、サービス証明書から公開鍵を抽出する。暗号化部１１０９は、データの暗号化を行う。

【００７０】

図１０の説明に戻って、秘匿化部６１７は、連結乱数のハッシュ値を算出する（Ｓ１０１１）。具体的には、図１１に示すように、算出部１１０１は、記憶部６０７から連結乱数を読み出し、連結乱数のハッシュ値を算出する。

【００７１】

図１０の説明に戻って、秘匿化部６１７は、コンテキストデータとハッシュ値を連結する（Ｓ１０１３）。具体的には、図１１に示すように、被署名データ生成部１１０３は、コンテキスト生成部６１１で生成されたコンテキストデータと、算出部１１０１で算出されたハッシュ値とを連結する。連結されたデータが、被署名データとなる。

【００７２】

図１０の説明に戻って、秘匿化部６１７は、署名を生成する（Ｓ１０１５）。具体的には、図１１に示すように、署名生成部１１０５は、格納部６１９からコンテキスト発行装置１０３の署名鍵を読み出し、被署名データ生成部１１０３で生成した被署名データに関する署名データを生成する。

【００７３】

図１０の説明に戻って、秘匿化部６１７は、公開鍵による暗号化を行う（Ｓ１０１７）。具体的には、図１１に示すように、抽出部１１０７は、記憶部６０７からサービス証明書を読み出し、サービス証明書から公開鍵を抽出する。公開鍵は、コンテキスト依存サーバ１０５の公開鍵である。そして、暗号化部１１０９は、公開鍵を用いて、署名データと被署名データとを暗号化する。その結果、署名データが暗号化された暗号化署名データと、被署名データが暗号化された暗号化被署名データとが生成される。但し、他の手順に従って、コンテキストを秘匿化するようにしてもよい。

【００７４】

図１０の説明に戻って、送信部６２１は、秘匿化コンテキストを送信する（Ｓ１０１９）。この例では、送信部６２１は、暗号化署名データと暗号化被署名データとを含む秘匿化コンテキストを利用者端末１０１に送信する（Ｓ１０２１）。

【００７５】

利用者端末１０１側で、受信部７０１は、秘匿化コンテキストを受信すると、秘匿化コンテキストをコンテキスト発行依頼部７１５に渡す。このようにして、コンテキスト発行依頼部７１５は秘匿化コンテキストを取得する。

【００７６】

図１２に、シーケンスの続きを示す。アクセスチケット取得部７１７は、コンテキスト依存サーバ１０５にアクセスを要求する（Ｓ１２０１）。具体的には、アクセスチケット取得部７１７は、記憶部７０９から連結乱数を読み取る。更に、アクセスチケット取得部７１７は、秘匿化コンテキストに含まれる暗号化署名データと暗号化被署名データと、連結乱数とを含むアクセス要求のデータを生成する。そして、送信部７０３から、コンテキスト依存サーバ１０５にアクセス要求のデータを送信する。つまり、伝送されるアクセス要求のデータには、暗号化署名データ、暗号化被署名データ及び連結乱数が含まれる（Ｓ

１２０３）。
【００７７】
コンテキスト依存サーバ１０５側で、受信部８０１がアクセス要求のデータを受信すると、アクセス要求のデータは、アクセスチケット発行部８０９に渡される。アクセスチケット発行部８０９は、アクセス要求のデータに含まれる暗号化署名データ、暗号化被署名データ及び連結乱数を記憶部８１１に記憶させる。
【００７８】
続いて、検証部８１３は、Ｓ１２０５乃至Ｓ１２１７の処理で、アクセス要求に関する検証を行う。
【００７９】
図１３に、検証部８１３の内部構成の例を示す。検証部８１３は、復号部１３０１、署名検証部１３０３、分離部１３０５、コンテキスト検証部１３０７、連結乱数検証部１３０９、再利用検出部１３１１及び時刻検証部１３１３を有している。
【００８０】
復号部１３０１は、暗号化されているデータを復号する。署名検証部１３０３は、電子署名を検証する処理を行う。分離部１３０５は、連結されているデータを分離する。コンテキスト検証部１３０７は、コンテキスト条件に従って、コンテキストを検証する。連結乱数検証部１３０９は、連結乱数を検証する。再利用検出部１３１１は、コンテキストの再利用を検出する。時刻検証部１３１３は、コンテキストに含まれる時刻を検証する。
【００８１】
図１２の説明に戻って、検証部８１３は、秘密鍵による復号を行う（Ｓ１２０５）。具体的には、図１３に示すように、復号部１３０１は、記憶部８１１から暗号化署名データと暗号化被署名データとを読み出し、更に、格納部８０７から秘密鍵を読み出す。そして、復号部１３０１は、暗号化署名データと暗号化被署名データとを、秘密鍵を用いて復号する。その結果、署名データと被署名データとが得られる。
【００８２】
図１２の説明に戻って、検証部８１３は、電子署名を検証する（Ｓ１２０７）。具体的には、図１３に示すように、署名検証部１３０３は、署名データの検証を行う。署名データの検証に成功した場合には、処理を続行する。署名データの検証に失敗した場合には、電子署名の検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。
【００８３】
図１２の説明に戻って、検証部８１３は、被署名データからコンテキストデータとハッシュ値とを分離する（Ｓ１２０９）。具体的には、図１３に示すように、分離部１３０５は、被署名データにおいて連結されているコンテキストデータとハッシュ値とを分離する。
【００８４】
図１２の説明に戻って、検証部８１３は、コンテキストを検証する（Ｓ１２１１）。具体的には、図１３に示すように、コンテキスト検証部１３０７は、格納部８０７からコンテキスト条件を読み出し、コンテキストデータがコンテキスト条件を満たしているか否かを判定する。コンテキストデータがコンテキスト条件を満たしていると判定した場合には、コンテキストの検証結果を成功とし、処理を続行する。コンテキストデータがコンテキスト条件を満たしていないと判定した場合には、コンテキストの検証結果を失敗とし、コンテキストの検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。
【００８５】
図１２の説明に戻って、検証部８１３は、連結乱数を検証する（Ｓ１２１３）。具体的には、図１３に示すように、連結乱数検証部１３０９は、記憶部８１１から連結乱数を読み出し、読み出した連結乱数のハッシュ値を算出する。そして、算出したハッシュ値と分離部１３０５で分離させたハッシュ値とを比較する。算出したハッシュ値と分離部１３０

５で分離させたハッシュ値とが一致すると判定した場合には、連結乱数の検証結果を成功とし、処理を続行する。算出したハッシュ値と分離部１３０５で分離させたハッシュ値とが一致しないと判定した場合には、連結乱数の検証結果を失敗とし、連結乱数の検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。

【００８６】

図１２の説明に戻って、検証部８１３は、コンテキストの再利用を検出する（Ｓ１２１５）。具体的には、図１３に示すように、再利用検出部１３１１は、分離部１３０５で分離させたハッシュ値が、ハッシュ値ＤＢ８１７に記憶されているハッシュ値のいずれかと一致するか否かを判定する。分離部１３０５で分離させたハッシュ値が、ハッシュ値ＤＢ８１７に記憶されているハッシュ値のいずれとも一致しないと判定した場合には、コンテキストの再利用ではないと判断する。そして、処理を続行する。分離部１３０５で分離させたハッシュ値が、ハッシュ値ＤＢ８１７に記憶されているハッシュ値のいずれかと一致すると判定した場合には、コンテキストの再利用であると判断する。そして、コンテキスト依存サーバ１０５は、コンテキストが再利用となることを利用者端末１０１に通知し、処理を中断する。

【００８７】

図１２の説明に戻って、検証部８１３は、時刻を検証する（Ｓ１２１７）。具体的には、図１３に示すように、時刻検証部１３１３は、コンテキストデータに含まれる時刻を特定する。そして、時刻検証部１３１３は、コンテキストデータ中の時刻と現在時刻の差分を算出する。差分は、コンテキストの生成時からの経過時間に相当する。そして、時刻検証部１３１３は、差分が閾値を越えているか否かを判定する。差分が閾値を越えていないと判定した場合には、時刻の検証結果を成功とし、処理を続行する。差分が閾値を越えていると判定した場合には、時刻の検証結果を失敗とし、時刻の検証に失敗したことを利用者端末１０１に通知する。そして、処理を中断する。

【００８８】

図１４に、シーケンスの続きを示す。上述の検証に成功すると、登録部８１５は、ハッシュ値をハッシュ値ＤＢ８１７に登録する（Ｓ１４０１）。

【００８９】

更に、コンテキスト依存サーバ１０５側で、アクセスチケット発行部８０９は、アクセスチケットを利用者端末１０１に送信する（Ｓ１４０３）。具体的には、アクセスチケット発行部８０９は、アクセスチケットを生成し、生成したアクセスチケットを格納部８０７に格納する。あるいは、アクセスチケット発行部８０９は、予め格納部８０７に格納されているアクセスチケットを読み出す。そして、送信部８０３からアクセスチケットが利用者端末１０１に送信される（Ｓ１４０５）。

【００９０】

利用者端末１０１側で、受信部７０１がアクセスチケットを受信すると、アクセスチケット取得部７１７は受信したアクセスチケットを受け取る。

【００９１】

利用者端末１０１側で、サービス取得部７１９は、サービスを要求する（Ｓ１４０７）。このとき、サービス取得部７１９は、送信部７０３を介してサービス要求のデータを送信する（Ｓ１４０９）。サービス要求のデータには、アクセスチケットが含まれる。

【００９２】

コンテキスト依存サーバ１０５側で、受信部８０１が、サービス要求のデータを受信すると、サービス要求のデータは、サービス提供部８１９に渡される。サービス提供部８１９は、判定部８２１にサービス要求のデータに含まれるアクセスチケットが正当であるか否かを判定させる（Ｓ１４１１）。アクセスチケットが正当でないと判定した場合には、アクセスチケットが正当でないことを利用者端末１０１に通知する。そして、処理を中断する。

【００９３】

アクセスチケットが正当であると判定した場合には、サービス提供部８１９は、サービ

スを提供する（Ｓ１４１３）。例えば、サービス提供部８１９は、受信部８０１からサービスに係るデータを送信する（Ｓ１４１５）。

【００９４】

本実施の形態によれば、利用者端末１０１から要求を受けたコンテキスト発行装置１０３側でコンテキストを生成し、更に署名を付するので、利用者端末１０１における不正なコンテキストの生成やコンテキストの改変を防止できる。

【００９５】

また、利用者端末１０１の信頼性に関わらず、安全にコンテキストに基づくネットワーク認証を行うことができる。

【００９６】

更に、コンテキスト依存サーバ１０５において、連結乱数のハッシュ値に基づき利用者端末１０１とコンテキスト発行装置１０３との組み合わせが正当であることを検証するので、他の装置によるコンテキストの流用を防止することができる。

【００９７】

更に、乱数表示に基づくペアリングを行うので、コンテキスト発行装置１０３から離れた場所にある装置からの不正なコンテキスト生成要求を排除することができる。

【００９８】

更に、コンテキスト発行装置１０３においてコンテキスト依存サーバ１０５の公開鍵によりコンテキストを暗号化するので、他のコンテキスト依存サーバ１０５によるコンテキストの転用を防ぐことができる。

【００９９】

更に、既に利用されているコンテキストと同じハッシュ値を有するコンテキストを検出するので、同一コンテキストの繰り返し利用を禁止することができる。

【０１００】

更に、サービス証明書を検証するので、コンテキスト依存サーバ１０５の成りすましを防止できる。

【０１０１】

更に、コンテキストに含まれる時刻を検証するので、生成から時間をあけて送られたコンテキストを無効とし、不正な時間差アクセスを排除できる。

【０１０２】

［実施の形態２］

上述した実施の形態では、コンテキスト発行装置１０３からコンテキストを利用者端末１０１に返し、利用者端末１０１からコンテキスト依存サーバ１０５にアクセスを要求するアプライアンス型のコンテキスト発行装置１０３について説明した。本実施の形態では、コンテキスト発行装置１０３からコンテキスト依存サーバ１０５にアクセスを要求し、取得したアクセスチケットを利用者端末１０１に転送するプロキシ型のコンテキスト発行装置１０３について説明する。

【０１０３】

システムの構成は、実施の形態１と同様である。

【０１０４】

図１５に、実施の形態２に係る装置間のデータフローの例を示す。コンテキスト発行装置１０３は、実施の形態１と同様に、コンテキスト発行装置１０３で生成した第１乱数を表示する（Ｓ１５０１）。利用者は、第１乱数を目視し、利用者端末１０１に入力する。第１乱数は、コンテキスト発行装置１０３に送られ、コンテキスト発行装置１０３で第１乱数を検証することによって、利用者端末１０１とコンテキスト発行装置１０３との間のペアリングが行われる。

【０１０５】

利用者端末１０１は、実施の形態１と同様に、コンテキスト依存サーバ１０５へサービス証明書を要求する（Ｓ１５０３）。コンテキスト依存サーバ１０５は、実施の形態１と同様に、利用者端末１０１からの要求に応じて、サービス証明書を利用者端末１０１に返

信する（Ｓ１５０５）。
【０１０６】
利用者端末１０１は、実施の形態１と同様に、コンテキスト発行装置１０３へコンテキストの発行を依頼する（Ｓ１５０７）。
【０１０７】
コンテキスト発行装置１０３は、種々の検証を行った上で、コンテキストを生成し、コンテキスト依存サーバ１０５にアクセスを要求する（Ｓ１５０９）。このとき、コンテキスト発行装置１０３は、秘匿化コンテキストを含むアクセス要求のデータをコンテキスト依存サーバ１０５に送信する。
【０１０８】
コンテキスト依存サーバ１０５は、秘匿化コンテキストについて種々の検証を行う。コンテキストが所定の条件を満たす場合に、認証成功と判定し、コンテキスト発行装置１０３に対してアクセスチケットを返信する（Ｓ１５１１）。
【０１０９】
コンテキスト発行装置１０３は、受け取ったアクセスチケットを利用者端末１０１に転送する（Ｓ１５１３）。
【０１１０】
利用者端末１０１は、実施の形態１と同様に、アクセスチケットを取得すると、そのアクセスチケットを送ることによって（Ｓ１５１５）、コンテキスト依存サーバ１０５で提供するサービスを受ける（Ｓ１５１７）。
【０１１１】
図１６に、実施の形態２に係るコンテキスト発行装置１０３のモジュール構成例を示す。図６に示した実施の形態１に係るコンテキスト発行装置１０３のモジュール構成例との相違点について説明する。記憶部６０７は、更にサーバアドレスを記憶する。サーバアドレスは、コンテキスト依存サーバ１０５のアドレスである。また、コンテキスト発行装置１０３は、更に転送部１６０１を有する。転送部１６０１は、受信部６０５からアクセスチケットを利用者端末１０１へ転送する。
【０１１２】
図１７に、実施の形態２に係る利用者端末１０１のモジュール構成例を示す。図７に示した実施の形態１に係る利用者端末１０１のモジュール構成例との相違点について説明する。
【０１１３】
コンテキスト発行依頼部７１５は、秘匿化コンテキストを受信しないので、受信部７０１との結線はない。また、アクセスチケット取得部７１７は、アクセスの要求を行わないので、送信部７０３との結線はない。
【０１１４】
利用者端末１０１のモジュール構成は、実施の形態１と同様である。
【０１１５】
図１８乃至２１に示したシーケンスに従って、実施の形態２に係る各装置の動作について説明する。図１８に示したシーケンスについて説明する。図１８に示したシーケンスは、図９に示した実施の形態１におけるシーケンスに対応する。Ｓ９０１乃至Ｓ９２３については、実施の形態１と同様である。
【０１１６】
利用者端末１０１側で、コンテキスト発行依頼部７１５は、コンテキスト発行装置１０３にコンテキスト発行を依頼する（Ｓ１８０１）。このとき、コンテキスト発行依頼部７１５は、コンテキス発行依頼のデータにサーバアドレスも含める（Ｓ１８０３）。
【０１１７】
図１９に示したシーケンスについて説明する。図１９に示したシーケンスは、図１０に示した実施の形態１におけるシーケンスに対応する。Ｓ１００１乃至Ｓ１０１７については、実施の形態１と同様である。

【０１１８】
コンテキスト発行装置１０３側で、送信部６２１は、コンテキスト依存サーバ１０５にアクセスを要求する（Ｓ１９０１）。具体的には、送信部６２１は、暗号化署名データと暗号化被署名データとを含むアクセス要求のデータをコンテキスト依存サーバ１０５に送信する（Ｓ１９０３）。本実施の形態に係るアクセス要求のデータには、実施の形態１で示したハッシュ値は含まれない。
【０１１９】
図２０に示したシーケンスについて説明する。図２０に示したシーケンスは、図１２に示した実施の形態１におけるコンテキスト依存サーバ１０５のシーケンスに対応する。Ｓ１２０５乃至Ｓ１２１７の処理のうち、連結乱数の検証（Ｓ１２１５）は行わない。コンテキスト発行装置１０３から利用者端末１０１へコンテキストを戻さないので、利用者端末１０１からコンテキストが流出することはない。従って、不正な装置からの要求を検出するための連結乱数の検証（Ｓ１２１５）は、省略するようにしてもよい。
【０１２０】
図２１に、に示したシーケンスについて説明する。図２１に示したシーケンスは、図１４に示した実施の形態１におけるシーケンスに対応する。
【０１２１】
Ｓ１４０１については、実施の形態１と同様である。コンテキスト依存サーバ１０５側で、アクセスチケット発行部８０９は、アクセスチケットをコンテキスト発行装置１０３に送信する（Ｓ２１０１）。伝送されるアクセスチケットは、実施の形態１と同様である（Ｓ２１０３）。
【０１２２】
コンテキスト発行装置１０３側の受信部６０５で受信されたアクセスチケットは、転送部１６０１に渡される。転送部１６０１は、送信部６２１を介してアクセスチケットを利用者端末１０１に送信する（Ｓ２１０５）。
【０１２３】
そして、利用者端末１０１の受信部７０１がアクセスチケットを受信する（Ｓ２１０７）。Ｓ１４０７乃至Ｓ１４１５については、実施の形態１と同様である。
【０１２４】
本実施の形態によれば、コンテキスト発行装置１０３から直接コンテキスト依存サーバ１０５へ秘匿化コンテキストを送るので、コンテキストの流出を防止することができる。
【０１２５】
上述の例では、表示された乱数を目視し、利用者が利用者端末１０１に入力する例を示したが、乱数に代えて不規則データに基づいて生成した幾何的コードを用いるようにしてもよい。例えば、コンテキスト発行装置１０３は幾何的コードを表示し、利用者端末１０１はカメラで幾何的コードを撮影し、不規則データを復元することによって、上述の乱数と同様に処理する。
【０１２６】
以上本技術の一実施の形態を説明したが、本技術はこれに限定されるものではない。例えば、上述の機能ブロック構成は実際のプログラムモジュール構成に一致しない場合もある。
【０１２７】
また、上で説明した各記憶領域の構成は一例であって、上記のような構成でなければならないわけではない。さらに、処理フローにおいても、処理結果が変わらなければ処理の順番を入れ替えることも可能である。さらに、並列に実行させるようにしても良い。
【０１２８】
図２２に、コンテキスト発行装置１０３のハードウエア構成例を示す。コンテキスト発行装置１０３は、ＲＡＭ２２０３、スピーカ２２０５、ＬＣＤ（Liquid Crystal Display：液晶ディスプレイ）２２０７、タッチパネル２２０９、マイク２２１１、ＮＡＮＤ（Not AND）メモリ２２１３、通信ＣＰＵ（Central Processing Unit）２２１５、アプリＣＰ

Ｕ２２１７、近距離通信デバイス２２１９、ＧＰＳ（Global Positioning System：全地球測位システム）センサー６３１、無線ＬＡＮ（Local Area Network）デバイス２２２３、ＤＳＰ（Digital Signal Processor）２２２５、ＩＳＰ（Image Signal Processor）２２２７、カメラ２２２９、バス２２３１、サブプロセッサ２２３３、地磁気センサー６３７、ジャイロセンサー６３５及び加速度センサー６３３を有している。そのうち、ＲＡＭ２２０３、スピーカ２２０５、ＬＣＤ２２０７、タッチパネル２２０９、マイク２２１１、ＮＡＮＤメモリ２２１３、通信ＣＰＵ２２１５、アプリＣＰＵ２２１７、近距離通信デバイス２２１９、ＧＰＳセンサー６３１、無線ＬＡＮデバイス２２２３、ＤＳＰ２２２５、ＩＳＰ２２２７及びカメラ２２２９は、バス２２３１を介して接続されている。ＬＣＤ２２０７は、表示装置の例である。

【０１２９】

ＲＡＭ２２０３は、例えばプログラムやデータを記憶する。スピーカ２２０５は、音声を出力する。ＬＣＤ２２０７は、画像や画面を表示する。タッチパネル２２０９は、接触状態と接触位置などを検出する。マイク２２１１は、音声を入力する。ＮＡＮＤメモリ２２１３は、不揮発性記憶素子のフラッシュメモリである。このＮＡＮＤメモリ２２１３は、例えばプログラムやデータを記憶する。通信ＣＰＵ２２１５は、通信処理に係る演算処理を行う。アプリＣＰＵ２２１７は、アプリケーションソフトを実行する演算装置である。近距離通信デバイス２２１９は、近距離通信を制御するデバイスである。ＧＰＳセンサー６３１は、位置を測定する装置である。無線ＬＡＮデバイス２２２３は、無線ＬＡＮの通信を制御するデバイスである。ＤＳＰ２２２５は、デジタル信号処理を行うプロセッサである。ＩＳＰ２２２７は、画像処理を行うプロセッサである。カメラ２２２９は、撮影する装置である。また、アプリＣＰＵ２２１７は、サブプロセッサ２２３３と接続している。サブプロセッサ２２３３は、地磁気センサー６３７、ジャイロセンサー６３５、及び加速度センサー６３３に接続している。サブプロセッサ２２３３は、地磁気センサー６３７、ジャイロセンサー６３５、及び加速度センサー６３３を制御する。地磁気センサー６３７とジャイロセンサー６３５は、姿勢角も測定する。

【０１３０】

この例では、アプリＣＰＵ２２１７は、サブプロセッサ２２３３を介して地磁気センサー６３７、ジャイロセンサー６３５、及び加速度センサー６３３の計測結果を取得するが、アプリＣＰＵ２２１７は、直接に地磁気センサー６３７、ジャイロセンサー６３５、及び加速度センサー６３３の計測結果を取得するようにしてもよい。

【０１３１】

また、上で述べたコンテキスト依存サーバ１０５は、コンピュータ装置であって、図２３に示すように、メモリ２５０１とＣＰＵ（Central Processing Unit）２５０３とハードディスク・ドライブ（ＨＤＤ：Hard Disk Drive）２５０５と表示装置２５０９に接続される表示制御部２５０７とリムーバブル・ディスク２５１１用のドライブ装置２５１３と入力装置２５１５とネットワークに接続するための通信制御部２５１７とがバス２５１９で接続されている。オペレーティング・システム（ＯＳ：Operating System）及び本実施例における処理を実施するためのアプリケーション・プログラムは、ＨＤＤ２５０５に格納されており、ＣＰＵ２５０３により実行される際にはＨＤＤ２５０５からメモリ２５０１に読み出される。ＣＰＵ２５０３は、アプリケーション・プログラムの処理内容に応じて表示制御部２５０７、通信制御部２５１７、ドライブ装置２５１３を制御して、所定の動作を行わせる。また、処理途中のデータについては、主としてメモリ２５０１に格納されるが、ＨＤＤ２５０５に格納されるようにしてもよい。本技術の実施例では、上で述べた処理を実施するためのアプリケーション・プログラムはコンピュータ読み取り可能なリムーバブル・ディスク２５１１に格納されて頒布され、ドライブ装置２５１３からＨＤＤ２５０５にインストールされる。インターネットなどのネットワーク及び通信制御部２５１７を経由して、ＨＤＤ２５０５にインストールされる場合もある。このようなコンピュータ装置は、上で述べたＣＰＵ２５０３、メモリ２５０１などのハードウエアとＯＳ及びアプリケーション・プログラムなどのプログラムとが有機的に協働することにより、上

で述べたような各種機能を実現する。

【０１３２】

以上述べた本発明の実施の形態をまとめると、以下のようになる。

【０１３３】

本実施の形態に係る情報処理装置は、コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、コンテキストを生成する第１の生成部と、コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、署名データと被署名データとを送信する送信部とを有する。

【０１３４】

このようにすれば、被認証装置から要求を受けた情報処理装置側でコンテキストを生成し、更に署名を付するので、被認証装置における不正なコンテキストの生成やコンテキストの改変を防止できる。

【０１３５】

上記情報処理装置は、更に、認証装置において被認証装置を検証するための情報とコンテキストとを含む被署名データを生成する第３の生成部を有するようにしてもよい。

【０１３６】

このようにすれば、認証装置における被認証装置の検証を補助し、他の装置によるコンテキストの流用を防止することに役立つ。

【０１３７】

また、上記送信部は、署名データと被署名データとを、認証装置へ送信するようにしてもよい。

【０１３８】

このようにすれば、コンテキストの流出を防止することができる。

【０１３９】

上記情報処理装置は、更に、不規則に生成されたデータを表示する表示部を有するようにしてもよい。また、上記情報処理装置は、不規則に生成されたデータを受信することにより、当該データの送信元である被認証装置を検証する第１の検証部を有するようにしてもよい。

【０１４０】

このようにすれば、情報処理装置から離れた場所にある装置からの不正なコンテキスト生成要求を排除することができる。

【０１４１】

上記情報処理装置は、更に、認証装置の公開鍵により、少なくとも被署名データを暗号化する暗号化部を有するようにしてもよい。

【０１４２】

このようにすれば、他の認証装置によるコンテキストの転用を防ぐことができる。

【０１４３】

本実施の形態に係る認証システムは、コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、コンテキストを生成する第１の生成部と、コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、署名データと被署名データとを送信する送信部とを有する情報処理装置と、署名データと被署名データとを受信すると、署名データに基づく検証を行う第１の検証部と、被署名データに含まれるコンテキストに対する検証を行う第２の検証部とを有する認証装置とを含む。

【０１４４】

このようにすれば、被認証装置の信頼性に関わらず、安全にコンテキストに基づくネットワーク認証を行うことができる。

【０１４５】

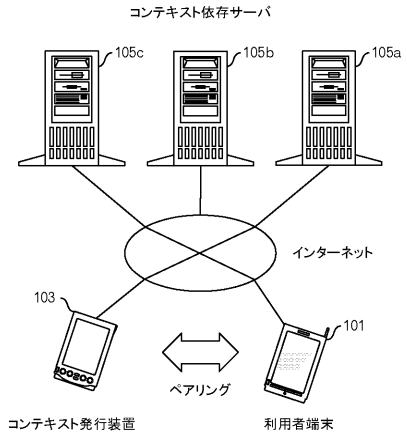
上記認証装置は、更に、　被署名データに含まれるコンテキスト固有のデータに基づいて、コンテキストの再利用を検出する検出部を有するようにしてもよい。

【０１４６】
このようにすれば、同一コンテキストの繰り返し利用を禁止することができる。
【０１４７】
なお、上記方法による処理をコンピュータに行わせるためのプログラムを作成することができ、当該プログラムは、例えばフレキシブルディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ、ハードディスク等のコンピュータ読み取り可能な記憶媒体又は記憶装置に格納されるようにしてもよい。尚、中間的な処理結果は、一般的にメインメモリ等の記憶装置に一時保管される。
【０１４８】
以上の実施例を含む実施形態に関し、さらに以下の付記を開示する。
【０１４９】
（付記１）
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成する第１の生成部と、
前記コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、
前記署名データと前記被署名データとを送信する送信部と
を有する情報処理装置。
【０１５０】
（付記２）
更に、
前記認証装置において前記被認証装置を検証するための情報と前記コンテキストとを含む前記被署名データを生成する第３の生成部
を有する付記１記載の情報処理装置。
【０１５１】
（付記３）
前記送信部は、前記署名データと前記被署名データとを、前記認証装置へ送信する
付記１又は２記載の情報処理装置。
【０１５２】
（付記４）
更に、
不規則に生成されたデータを表示する表示部と、
前記不規則に生成されたデータを受信することにより、当該データの送信元である前記被認証装置を検証する第１の検証部と
を有する付記１乃至３のいずれか１つ記載の情報処理装置。
【０１５３】
（付記５）
更に、
前記認証装置の公開鍵により、少なくとも前記被署名データを暗号化する暗号化部
を有する付記１乃至４のいずれか１つ記載の情報処理装置。
【０１５４】
（付記６）
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成する第１の生成部と、
前記コンテキストを含む被署名データに対する署名データを生成する第２の生成部と、
前記署名データと前記被署名データとを送信する送信部と
を有する情報処理装置と、
前記署名データと前記被署名データとを受信すると、前記署名データに基づく検証を行う第１の検証部と、
前記被署名データに含まれる前記コンテキストに対する検証を行う第２の検証部と
を有する認証装置と

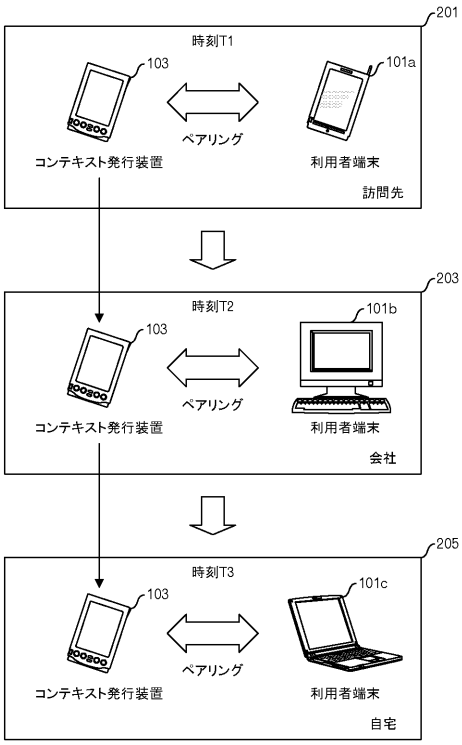
を含む認証システム。
【０１５５】
（付記７）
前記認証装置は、更に、
前記被署名データに含まれるコンテキスト固有のデータに基づいて、前記コンテキストの再利用を検出する検出部
を有する付記８記載の認証システム。
【０１５６】
（付記８）
コンテキストに基づくネットワーク認証を行う認証装置にアクセスしようとする被認証装置からの要求に応じて、前記コンテキストを生成し、
前記コンテキストを含む被署名データに対する署名データを生成し、
前記署名データと前記被署名データとを送信する
処理をコンピュータに実行させるためのプログラム。
【符号の説明】
【０１５７】
１０１　利用者端末　　１０３　コンテキスト発行装置
１０５　コンテキスト依存サーバ
２０１　訪問先　　２０３　会社
２０５　自宅　　３０１　施設
４０１　会場　　６０１　乱数生成部
６０３　表示部　　６０５　受信部
６０７　記憶部　　６０９　検証部
６１１　コンテキスト生成部　　６１３　センサー群
６１５　時計部　　６１７　秘匿化部
６１９　格納部　　６２１　送信部
６３１　ＧＰＳセンサー　　６３３　加速度センサー
６３５　ジャイロセンサー　　６３７　地磁気センサー
７０１　受信部　　７０３　送信部
７０５　受付部　　７０７　サービス証明書取得部
７０９　記憶部　　７１１　検証部
７１３　乱数生成部　　７１５　コンテキスト発行依頼部
７１７　アクセスチケット取得部　　７１９　サービス取得部
８０１　受信部　　８０３　送信部
８０５　サービス証明書発行部　　８０７　格納部
８０９　アクセスチケット発行部　　８１１　記憶部
８１３　検証部　　８１５　登録部
８１７　ハッシュ値ＤＢ　　８１９　サービス提供部
８２１　判定部　　１１０１　算出部
１１０３　被署名データ生成部　　１１０５　署名生成部
１１０７　抽出部　　１１０９　暗号化部
１３０１　復号部　　１３０３　署名検証部
１３０５　分離部　　１３０７　コンテキスト検証部
１３０９　連結乱数検証部　　１３１１　再利用検出部
１３１３　時刻検証部　　１６０１　転送部
２２０３　ＲＡＭ　　２２０５　スピーカ
２２０７　ＬＣＤ　　２２０９　タッチパネル
２２１１　マイク　　２２１３　ＮＡＮＤメモリ
２２１５　通信ＣＰＵ　　２２１７　アプリＣＰＵ
２２１９　近距離通信デバイス　　２２２３　無線ＬＡＮデバイス

２２２５　ＤＳＰ　　２２２７　ＩＳＰ
２２２９　カメラ　　２２３１　バス
２２３３　サブプロセッサ

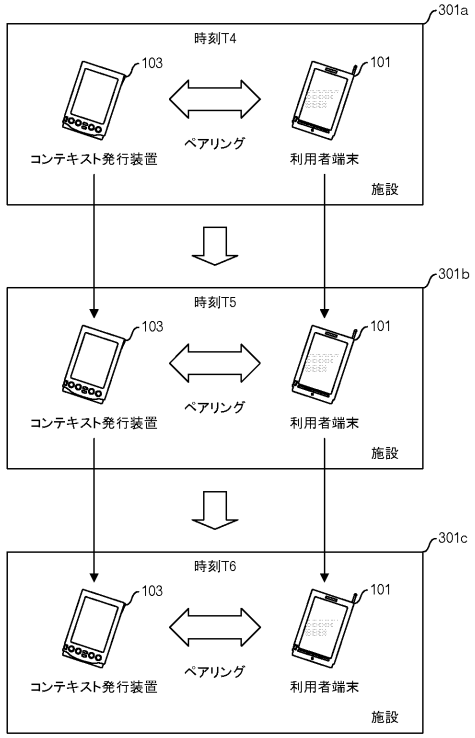
【図１】



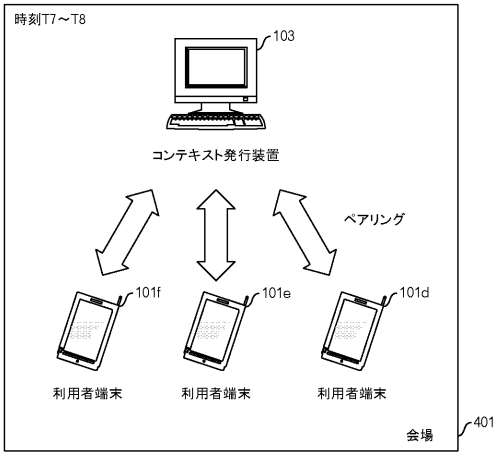
【図２】



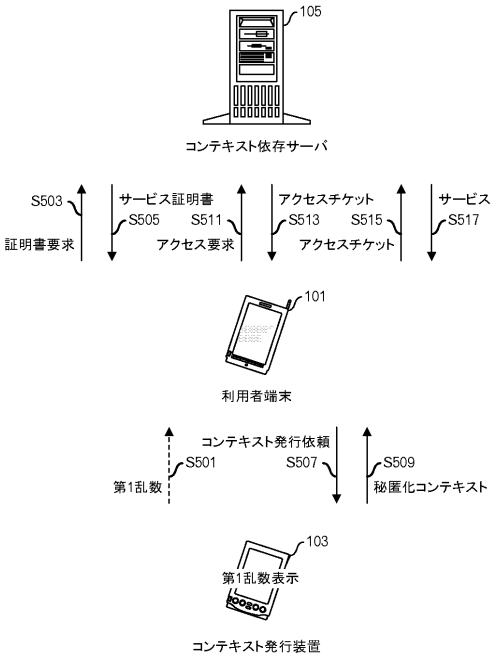
【図３】


301a
時刻T4
103
101
ペアリング
コンテキスト発行装置
利用者端末
施設
301b
時刻T5
103
101
ペアリング
コンテキスト発行装置
利用者端末
施設
301c
時刻T6
103
101
ペアリング
コンテキスト発行装置
利用者端末
施設

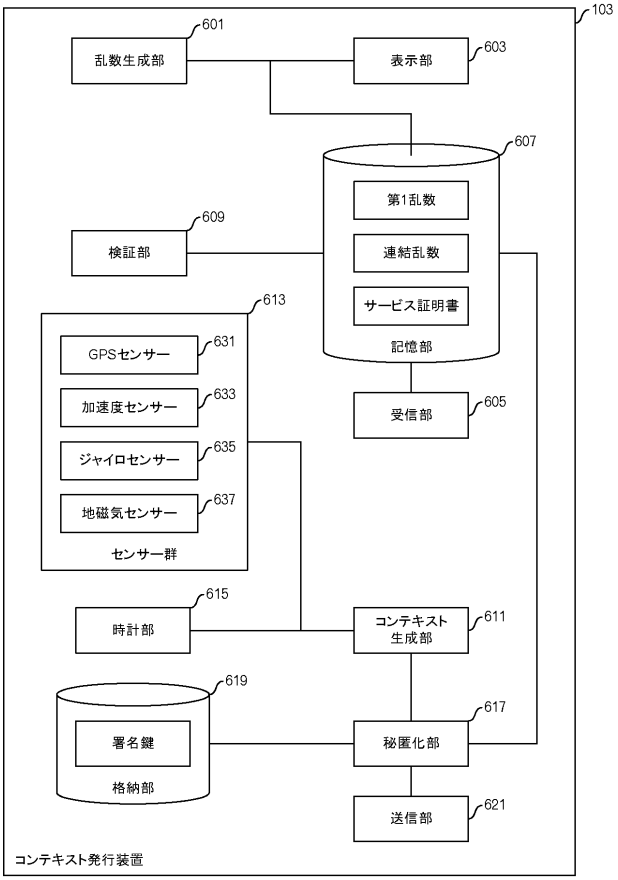
【図４】


時刻T7～T8
103
コンテキスト発行装置
ペアリング
101f
101e
101d
利用者端末
利用者端末
利用者端末
会場
401

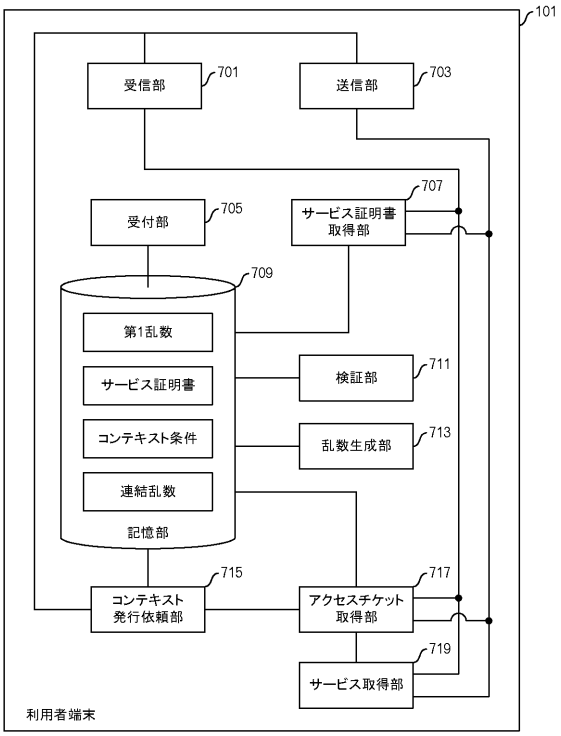
【図５】


105
コンテキスト依存サーバ
S503
証明書要求
サービス証明書
S505
S511
アクセス要求
アクセスチケット
S513
S515
アクセスチケット
サービス
S517
101
利用者端末
コンテキスト発行依頼
S501
S507
S509
第1乱数
秘匿化コンテキスト
103
第1乱数表示
コンテキスト発行装置

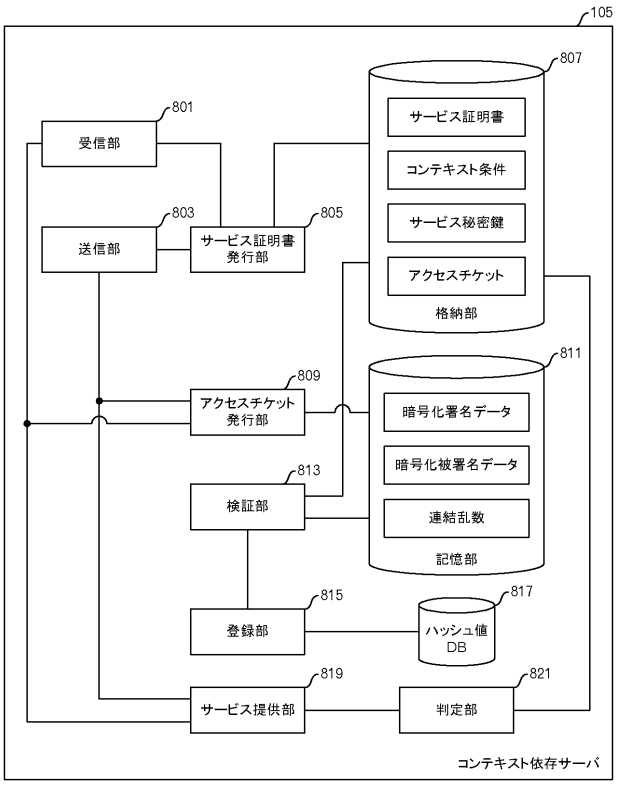
【図６】


103
601
乱数生成部
603
表示部
607
第1乱数
連結乱数
サービス証明書
記憶部
609
検証部
613
GPSセンサー
631
加速度センサー
633
ジャイロセンサー
635
地磁気センサー
637
センサー群
605
受信部
615
時計部
611
コンテキスト
生成部
619
署名鍵
格納部
617
秘匿化部
621
送信部
コンテキスト発行装置

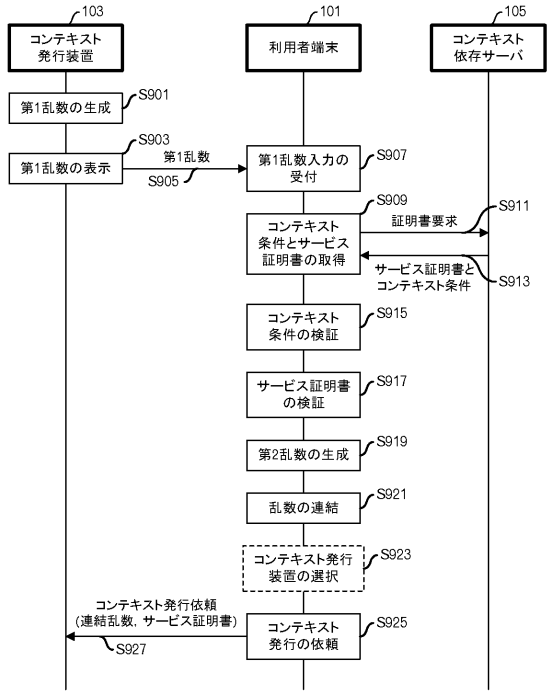
【図７】


101
受信部
701
送信部
703
受付部
705
サービス証明書取得部
707
709
第1乱数
サービス証明書
コンテキスト条件
連結乱数
記憶部
検証部
711
乱数生成部
713
コンテキスト発行依頼部
715
アクセスチケット取得部
717
サービス取得部
719
利用者端末

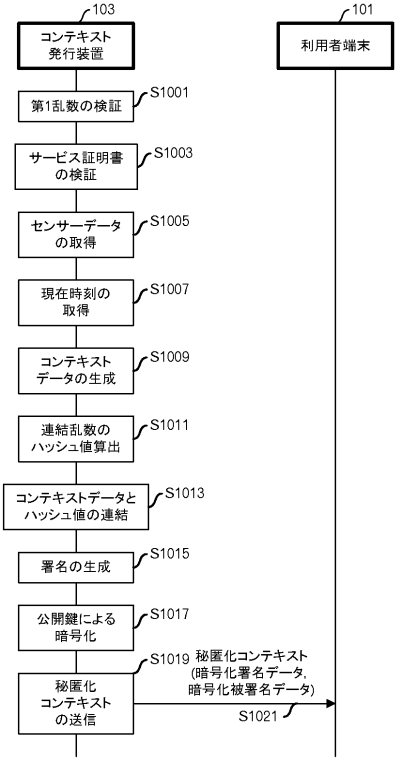
【図８】


105
807
サービス証明書
コンテキスト条件
サービス秘密鍵
アクセスチケット
格納部
801
受信部
803
送信部
サービス証明書発行部
805
811
暗号化署名データ
暗号化被署名データ
連結乱数
記憶部
809
アクセスチケット発行部
813
検証部
815
登録部
817
ハッシュ値DB
819
サービス提供部
821
判定部
コンテキスト依存サーバ

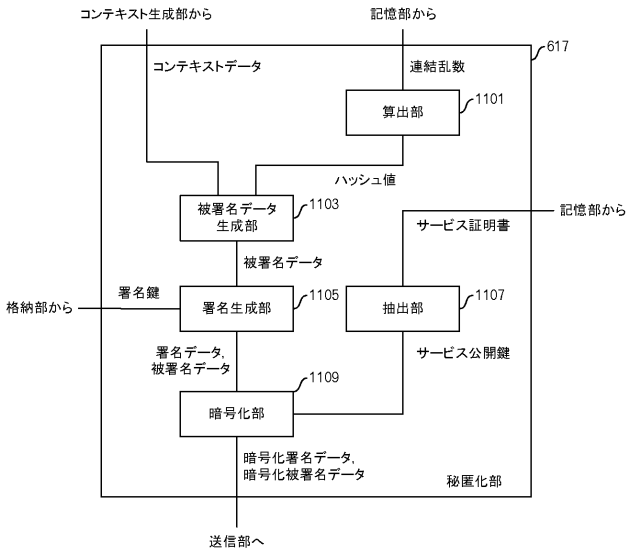
【図９】


103
コンテキスト発行装置
101
利用者端末
105
コンテキスト依存サーバ
第1乱数の生成
S901
第1乱数の表示
S903
第1乱数
S905
第1乱数入力の受付
S907
S909
コンテキスト条件とサービス証明書の取得
証明書要求
S911
サービス証明書とコンテキスト条件
S913
コンテキスト条件の検証
S915
サービス証明書の検証
S917
第2乱数の生成
S919
乱数の連結
S921
コンテキスト発行装置の選択
S923
コンテキスト発行依頼
(連結乱数，サービス証明書)
S927
コンテキスト発行の依頼
S925

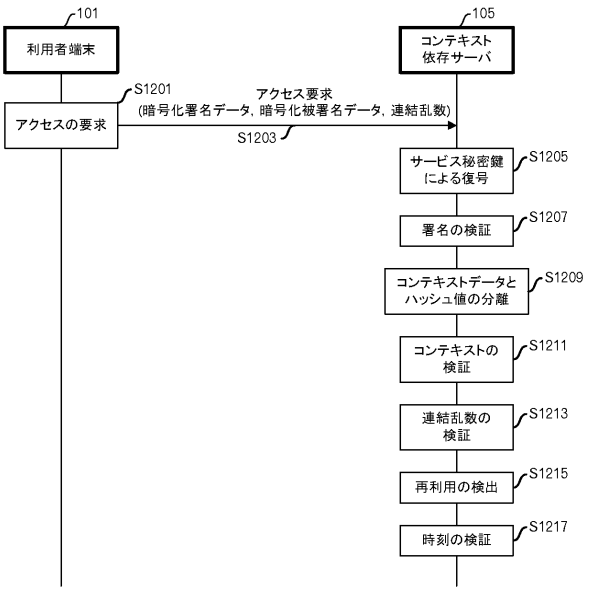
【図１０】


103
コンテキスト発行装置
101
利用者端末
第1乱数の検証
S1001
サービス証明書の検証
S1003
センサーデータの取得
S1005
現在時刻の取得
S1007
コンテキストデータの生成
S1009
連結乱数のハッシュ値算出
S1011
コンテキストデータとハッシュ値の連結
S1013
署名の生成
S1015
公開鍵による暗号化
S1017
秘匿化コンテキストの送信
S1019
秘匿化コンテキスト
(暗号化署名データ，暗号化被署名データ)
S1021

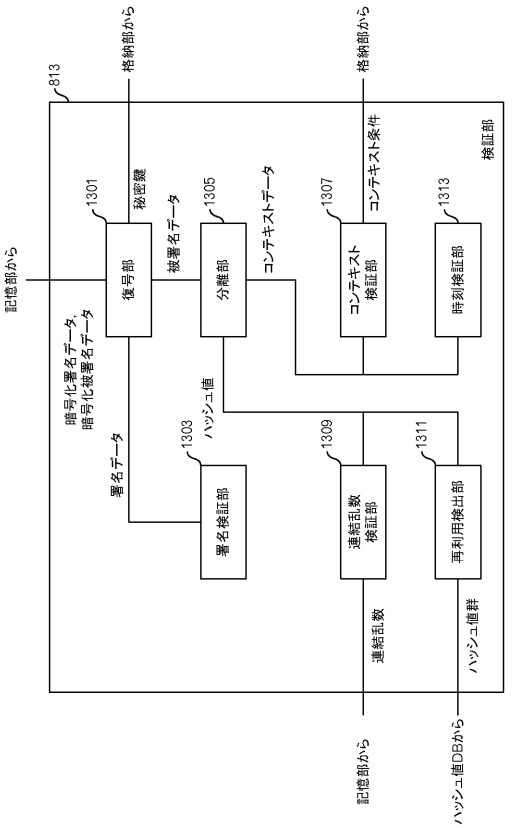
【図１１】



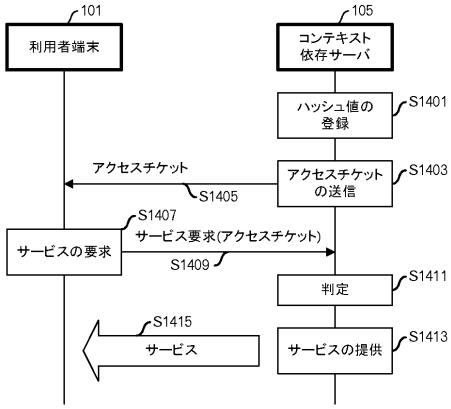
【図１２】



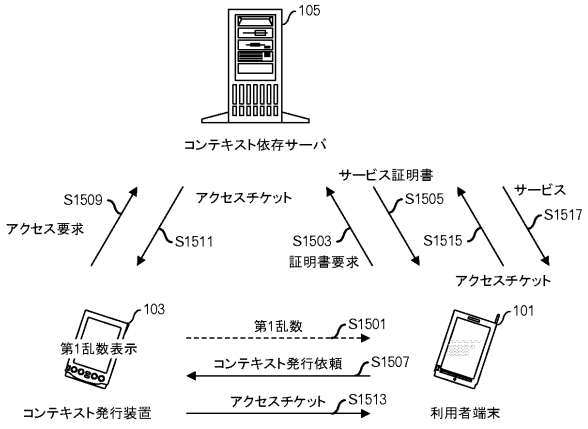
【図１３】



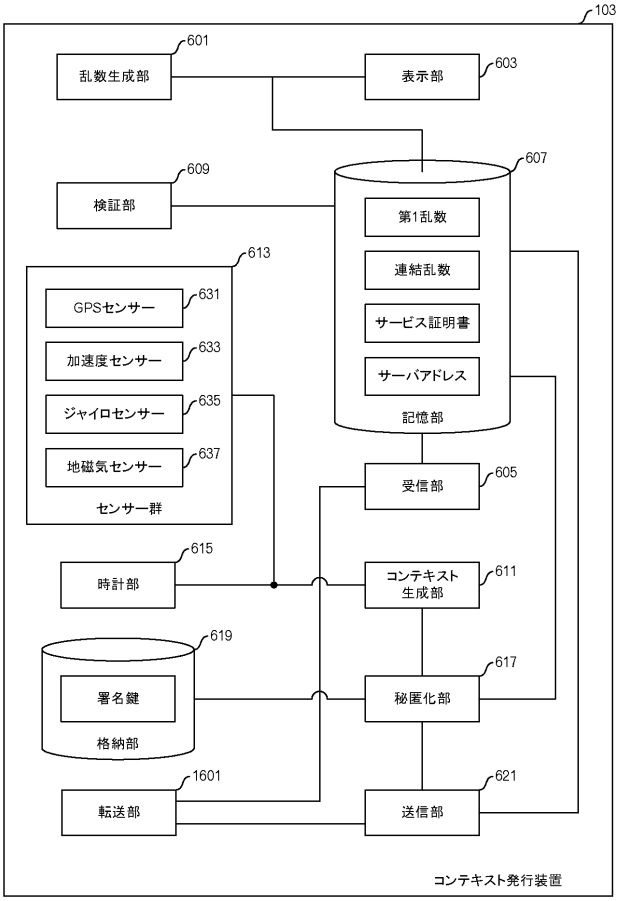
【図１４】



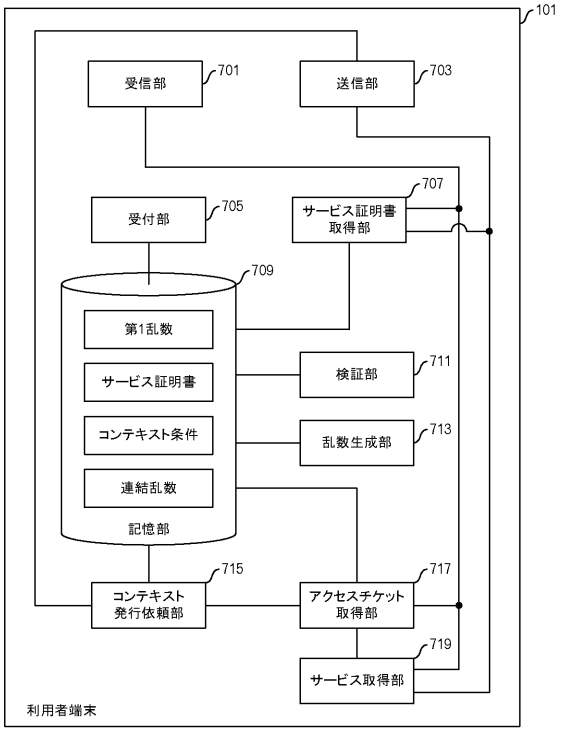
【図１５】



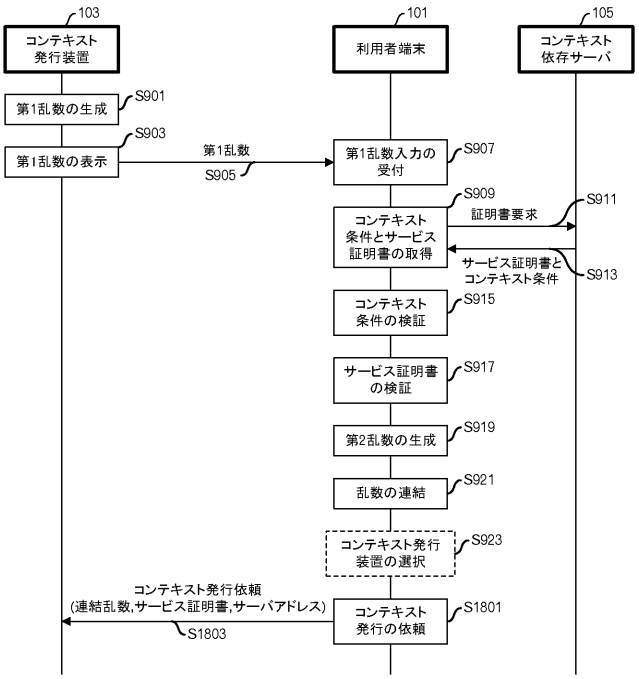
【図１６】



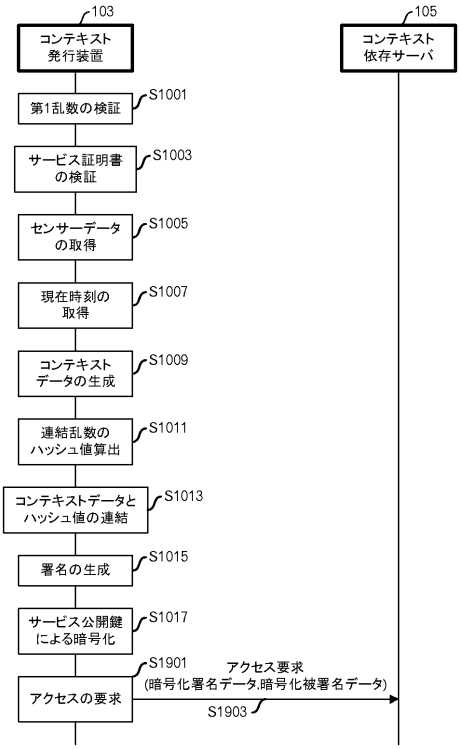
【図１７】



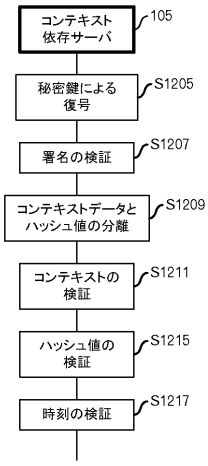
【図１８】



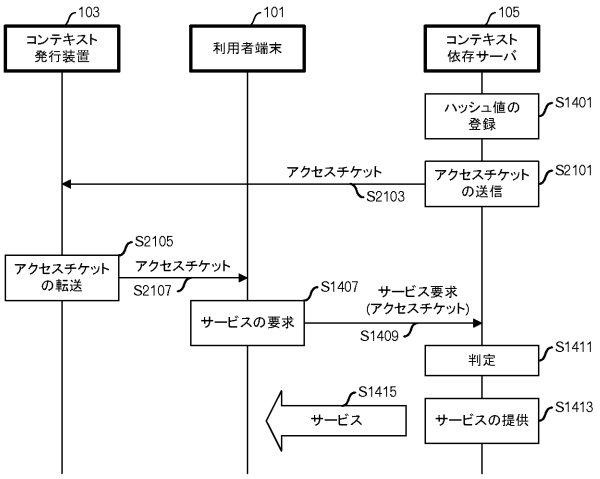
【図１９】



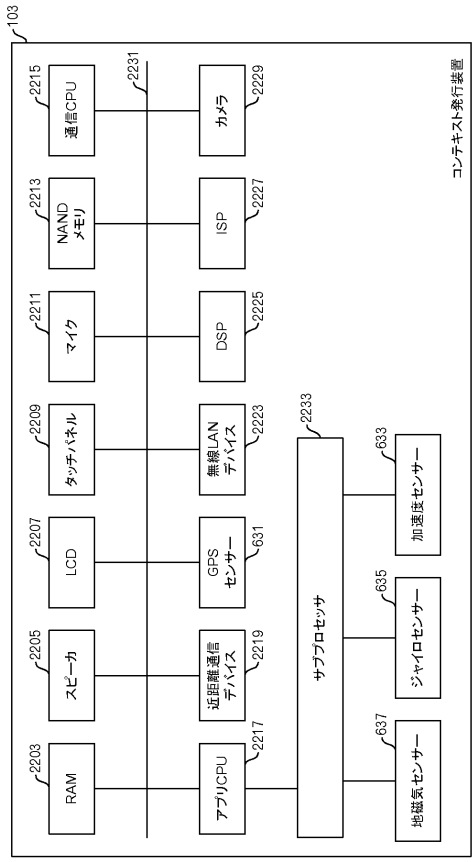
【図２０】



【図２１】



【図２２】



【図２３】