(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4372446号
(P4372446)
(45)発行日　平成21年11月25日(2009.11.25)　(24)登録日　平成21年9月11日(2009.9.11)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 520E
H04L 9/32 (2006.01)　　H04L 9/00 675B
G06F 21/20 (2006.01)　　G06F 15/00 330B

請求項の数 3　(全 15 頁)

(21)出願番号　特願2003-111096(P2003-111096)
(22)出願日　平成15年4月16日(2003.4.16)
(65)公開番号　特開2004-7589(P2004-7589A)
(43)公開日　平成16年1月8日(2004.1.8)
審査請求日　平成18年4月5日(2006.4.5)
(31)優先権主張番号　10/063,361
(32)優先日　平成14年4月16日(2002.4.16)
(33)優先権主張国　米国(US)

(73)特許権者　596170170
ゼロックス　コーポレイション
ＸＥＲＯＸ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国、コネチカット州　０６８５６、ノーウォーク、ピーオーボックス　４５０５、グローバー・アヴェニュー　４５
(74)代理人　100075258
弁理士　吉田　研二
(74)代理人　100096976
弁理士　石田　純
(72)発明者　マーク　ストリンガー
イギリス　ケンブリッジ　スタッフォードシャー　ストリート　シェンストーン　ハウス　５

最終頁に続く

(54)【発明の名称】文書およびサービスへの安全なアドホックアクセス

(57)【特許請求の範囲】
【請求項１】
ネットワーク上に位置する文書サーバの登録ユーザである第１のユーザが、前記文書サーバの登録ユーザではない第２のユーザに対して、前記文書サーバ上に保存した電子文書またはサービスへの安全なアクセスを付与する方法であって、前記第１のユーザと、前記第２のユーザと、前記文書サーバとは対応の秘密鍵が関連付けられた公開鍵でそれぞれ関連付けられ、前記文書サーバ上で実行される前記方法は、
前記第１のユーザと公開鍵を交換して第１の安全なセッションを確立するステップと、
前記第１のユーザからファイルディレクトリのリストに対するリクエストを受信し、前記第１の安全なセッションの確立時に前記第１のユーザから付与された信用証明書を用いて前記第１のユーザの前記ファイルディレクトリに対するリクエストを認証するステップと、
前記第１のユーザに前記ファイルディレクトリのリストを前記第１の安全なセッションで送信するステップであって、前記リストは前記文書サーバ上で利用可能なコンテンツへのパスの組を特定するステップと、
前記第２のユーザと公開鍵を交換して第２の安全なセッションを確立するステップと、
前記第２のユーザから前記文書サーバ上の選択コンテンツへのアクセスリクエストを受信するステップであって、前記アクセスリクエストはトークン識別子を含み、前記トークン識別子は、前記文書サーバに記録され、かつ前記文書サーバ上で利用可能なコンテンツへの前記パスの組のうち前記選択コンテンツへのパスに関連付けられるステップと、

（ａ）前記第２の安全なセッションの確立時に前記第２のユーザから受信した前記第２のユーザの公開鍵と、（ｂ）前記第２のユーザの前記公開鍵と前記文書サーバ上の前記選択コンテンツへの前記アクセスリクエストの他の関連情報との署名入り暗号要約である、前記第１のユーザの前記秘密鍵を用いて署名したデジタル署名とを用いて、前記アクセスリクエストを認証するステップと、
前記アクセスリクエストが認証されれば、前記第２のユーザに前記第２の安全なセッションで前記選択コンテンツへのアクセスを付与するステップとを含むアクセス権付与方法。
【請求項２】
請求項１に記載のアクセス権付与方法であって、
前記第１のユーザから、前記文書サーバ上で利用可能な前記選択コンテンツへのパスに関連付けられるトークンを作成するリクエストを受信するステップと、
前記文書サーバ上のトークンデータベース中で、前記トークン識別子が関連付けられた前記トークンを作成するステップと、
前記第１のユーザに、前記トークンデータベース中の前記トークンを固有（ユニーク）に特定する前記トークン識別子を安全なセッションで送信するステップとをさらに含むアクセス権付与方法。
【請求項３】
文書サーバであって、前記文書サーバは、ネットワーク上に位置する前記文書サーバの登録ユーザである第１のユーザが、前記文書サーバの登録ユーザではない第２のユーザに対して、前記文書サーバ上に保存した電子文書またはサービスへの安全なアクセス権を付与するアクセス権付与プログラムを実行し、前記第１のユーザと、前記第２のユーザと、前記文書サーバとは、対応の秘密鍵をもつ公開鍵でそれぞれ関連付けられ、前記文書サーバは、
命令を記憶するメモリと、
前記メモリに接続されて、前記文書サーバの前記命令を実行するプロセッサとを含み、前記プロセッサは前記命令の実行時に、
前記第１のユーザと公開鍵を交換して第１の安全なセッションを確立するステップと、
前記第１のユーザからファイルディレクトリのリストに対するリクエストを受信し、前記第１の安全なセッションの確立時に前記第１のユーザから付与された信用証明書を用いて前記第１のユーザの前記ファイルディレクトリに対するリクエストを認証するステップと、
前記第１のユーザに前記ファイルディレクトリのリストを前記第１の安全なセッションで送信するステップであって、前記リストは前記文書サーバ上で利用可能なコンテンツへのパスの組を特定するステップと、
前記第２のユーザと公開鍵を交換して第２の安全なセッションを確立するステップと、
前記第２のユーザから前記文書サーバ上の選択コンテンツへのアクセスリクエストを受信するステップであって、前記アクセスリクエストはトークン識別子を含み、前記トークン識別子は、前記文書サーバに記録され、かつ前記文書サーバ上で利用可能なコンテンツへの前記パスの組のうち前記選択コンテンツへのパスに関連付けられるステップと、
（ａ）前記第２の安全なセッションの確立時に前記第２のユーザから受信した前記第２のユーザの公開鍵と、（ｂ）前記第２のユーザの前記公開鍵と前記文書サーバ上の前記選択コンテンツへの前記アクセスリクエストの他の関連情報との署名入り暗号要約である、前記第１のユーザの前記秘密鍵を用いて署名したデジタル署名とを用いて、前記リクエストを認証するステップと、
前記アクセスリクエストが認証されれば、前記第２のユーザに前記第２の安全なセッションで前記選択コンテンツへのアクセスを付与するステップとを行う文書サーバ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は一般には、ファイアウォールで保護されたネットワーク上に保存された文書また

はサービスに対して、ネットワークの登録ユーザではない、ファイアウォール外に位置するユーザに安全なアクセスを付与する方法、装置およびシステムに関する。

【０００２】

【従来の技術】

現在、私設ネットワークのファイアウォールの内に保存された多くの文書およびサービスを、私設ネットワークへのアクセス権をもたない（すなわち私設ネットワーク上の登録ユーザではない）ユーザが共有することが求められている。私設ネットワークとは、ネットワークのゲートウェイまたは各マシンにおいてネットワークへのアクセスを制限する任意のネットワークをさす。

【０００３】

一般に、ネットワークはゲートウェイを介して他のネットワークに接続される。ゲートウェイにはファイアウォールが設置され、未認可のアクセスがゲートウェイを通過することを防止する。例えば、私設ネットワークは、ゲートウェイを介してインターネット等の公設ネットワークに接続される企業内イントラネットとして構成してもよい。私設ネットワークのゲートウェイには、私設ネットワークとの間でやりとりされるメッセージをチェックするファイアウォールを設置できる。メッセージは、所定のセキュリティ基準（発信元が特定アドレス、宛先が特定ポート等）に合致した場合にのみ、ファイアウォールを通過する。

【０００４】

従って、私設ネットワークに事前登録していないユーザは、私設ネットワークのファイアウォールで保護された文書およびサービスにアクセスすることができない。

【０００５】

【発明が解決しようとする課題】

本発明は、上記課題に鑑みてなされたものであり、その目的は、私設ネットワークに事前登録していないユーザに、私設ネットワークのファイアウォールで保護された文書、ダイナミックな情報およびサービスへアクセスできる制御された安全なアクセス権を付与する方法、装置ならびにシステムを提供することである。

【０００６】

【課題を解決するための手段】

本発明に従い、ネットワーク上に位置する文書サーバの登録ユーザである第１のユーザが、該文書サーバの登録ユーザではない第２のユーザに対して、該文書サーバに保存した電子文書またはサービスへの安全なアクセス権を付与する方法、システム、および製造物（プログラムを含む）を提供する。第１のユーザと、第２のユーザと、文書サーバとは、それぞれ公開鍵で関連付けられており、公開鍵には対応する秘密鍵が関連付けられる。文書サーバ上で実行される方法は、

第１のユーザと公開鍵を交換して、第１の安全なセッションを確立するステップと、

第１のユーザからファイルディレクトリをリストするリクエストを受信するステップと、

第１の安全セッション確立時に第１のユーザから付与された信用証明書を用いて、第１のユーザのファイルディレクトリに対するリクエストを認証するステップと、

第１のユーザに、文書サーバ上で利用可能なコンテンツへのパスの組を特定するファイルディレクトリのリストを第１の安全なセッションで送信するステップと、

第２のユーザと公開鍵を交換して第２の安全なステップを確立するステップと、

第２のユーザから文書サーバ上の選択コンテンツへのアクセスリクエストを受信するステップであって、アクセスリクエストはトークン識別子を含み、該トークン識別子は、文書サーバに記録され、かつ文書サーバ上で利用可能なコンテンツへのパスの組のうち選択コンテンツへのパスに関連付けられるステップと、

（ａ）第２の安全なセッション確立時に第２のユーザから受信した第２のユーザの公開鍵と、（ｂ）第２のユーザの公開鍵と文書サーバ上の選択コンテンツへのアクセスリクエストの他の関連情報（トークン識別子、選択コンテンツへのパス、作成日、アクセス権等）との署名入り暗号要約である、第１のユーザの秘密鍵を用いて署名したデジタル署名とを

用いて、アクセスリクエストを認証するステップと、
および、アクセスリクエストが認証されれば、第２のユーザに第２の安全なセッションで選択コンテンツへのアクセス権を付与するステップとを含む文書サーバである。

【０００７】

【発明の実施の形態】

図１は、本発明を実行する動作環境１００を示す。この動作環境は文書サーバ１０２を含み、これはインターネット１０４等の（有線または無線）公設ネットワークおよび／または信頼できないネットワークを介して、ユーザデバイスＡ１０６およびユーザデバイスＢ１０８（それぞれユーザＡおよびユーザＢとも称す）と直接または間接的に通信する。ユーザデバイス１０６および１０８は、ハンドヘルドデバイス、ラップトップコンピュータ、デスクトップコンピュータおよびサーバ等の可動または固定計算装置で構成できる。

【０００８】

一実施形態では、各公開鍵は、各当事者（第１のユーザ、第２のユーザ、または文書サーバ等）が保持するデジタル証明書の一部として含まれ、各当事者はデジタル証明書に関連した秘密鍵を保有する。

【０００９】

本発明の上記およびそれ以外の各アスペクト（特徴）は、添付図面を参照して以下の説明から明白となる。図面中、同一参照番号は同一箇所をさす。

【００１０】

文書サーバ１０２は、ファイアウォール１１２で保護された私設ネットワーク１１４（イントラネット等）のゲートウェイ１１０を介して、ユーザデバイス１０６および／または１０８と間接的に通信する。本実施形態または他の実施形態では、プロキシサーバ１１６（またはプロキシ１１６）を用いて、文書サーバ１０２との通信をフィルタしてもよい。さらに他の実施形態では、文書サーバ１０２は、信頼できるまたはできないネットワークを介してデバイス１０６および／または１０８と直接通信する。

【００１１】

動作環境１００はまた、公開鍵基盤（ＰＫＩ）を含む。一般にＰＫＩでは、証明書発行機関１１８または信頼された第三者によって文書サーバ１０２に発行されるデジタル証明書１２０、デバイス１０６のユーザＡに発行されるデジタル証明書１３２、およびデバイス１０８のユーザＢに発行されるデジタル証明書１３４に署名が行われる。公開鍵基盤では、デジタル証明書を使用することによって当事者双方が事前に関係を持つことなく互いに安全な通信をダイナミックに確立できる。

【００１２】

デジタル証明書は、例えばＩＴＵ　Ｘ．５０９デジタル証明書標準に記載される形式で構成される。または、デジタル証明書はＷＡＰ（無線アプリケーションプロトコル）のＷＴＬＳ（無線トランスポート層セキュリティ）セキュリティ層に記載される形式、もしくはＳＰＫＩ（シンプル公開鍵基盤）証明書の形式で構成してもよい。

【００１３】

本発明を実行するには、ＲＳＡ（リベストRivest－シャミアShamir－エーデルマンAdleman）公開鍵暗号技術以外の他の暗号方式、例えば楕円曲線暗号方式もしくは米国デジタル署名標準（ＤＳＳ－Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）のデジタル署名アルゴリズム（ＤＳＡ－Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ｓｔａｎｄａｒｄ）構成部分等を用いてもよい。

【００１４】

動作環境１００では１つまたは複数の証明書発行機関を使用してもよい。例えば、私設ネットワーク１１４がネットワークの認可ユーザに発行する証明書をサービスする独自の証明書発行機関を有してもよいし、または一部またはすべての関係者（ユーザＡ、ユーザＢ、文書サーバ等）が一般の認可証明書発行サービス局（Ｖｅｒｉｓｉｇｎ（登録商標）等）から証明書を入手してもよい。最後に、文書サーバはデジタル証明書に誰が署名したかではなく、鍵に基づいて信頼すべきエンティティティ（実体）を認識すること、かつ自署

証明書（つまりキーペアの帰属先が自身の証明書発行機関として機能する場合）等の任意証明書または未署名の公開鍵を単独で用いてもよいことが、当業者には明白と考える。

【００１５】

二者（例えばユーザＡと文書サーバ）が自身の公開鍵を交換して、それを個々の秘密鍵と組み合わせると、当事者双方は特定の通信セッション用の対称秘密鍵（すなわちセッションキー）についての合意ができる。セッションキーは、二者間で安全ではない（すなわち信頼できない）通信チャネルを介して送信される情報の暗号化および復号化に使用される。このようにセッションキーを定義することにより、二者が通信する通信チャネルを傍受者が観察してセッションキーを推定することを不可能にする。

【００１６】

上記の方法で安全ではない通信チャネルを介してデータを安全に送信するためのプロトコルの一つが、１９９６年3月4日発行の”Ｔｈｅ　ＳＳＬ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ　３．０”に記載のＳｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ（ＳＳＬ）プロトコルで定義されている。他の実施形態では、ＳＳＬをベースにしたＴｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ（ＴＬＳ）という名称のインターネット・エンジニアリング・タスクフォース（ＩＥＴＦ）標準を用いて、インターネットによる安全なセッションを確立することもできる。ＴＬＳはＩＥＴＦ　ＲＦＣ２２４６として記載されている。ＳＳＬ３．０プロトコルとＴＬＳプロトコルとは標準的なウェブブラウザでサポートされ、拡張子「ｈｔｔｐｓ」を用いるハイパーテキスト転送プロトコル（ＨＴＴＰ）の一部として起動される。

【００１７】

公開鍵基盤の一側面に従って、文書サーバ１０２と、ユーザＡデバイス１０６と、ユーザＢデバイス１０８とは、選択したコンテンツのデジタル署名を作成するように適合される。デジタル署名は、所与の秘密鍵を用いた選択コンテンツの署名入りの暗号要約である。この所与の秘密鍵に対応する公開鍵をもつものは誰でも、この署名入りの暗号要約の真正さを証明できる。公開鍵基盤の他の側面に従えば、文書サーバ１０２と、ユーザＡデバイス１０６と、ユーザＢデバイス１０８とは、各者間で確立される各通信セッション（すなわち安全なセッション）用のセッションキーを定義するように適合される。

【００１８】

一般に、文書サーバは、文書サーバの未登録ユーザ（例えばユーザＢ）が操作するクライアントデバイスに対して、ファイアウォールで保護された文書またはサービスへの安全なアドホックアクセスを提供するように適合される。クライアントデバイスは、ＰＤＡ（携帯情報端末）、スマートフォン、およびラップトップ等の可動装置で構成できる。文書サーバはクライアントデバイス上で動作する既存のブラウザとシームレスで通信し、特別な操作は必要に応じてブラウザによってリアルタイムでクライアントデバイスにダウンロードされるため、カスタム仕様のソフトウェアをクライアントデバイス、ファイアウォール、またはプロキシサーバに設置しなくてもよいという利点がある。

【００１９】

文書サーバ１０２は、該サーバ上、または該サーバが通信アクセスを有する１台以上のサーバ上に保存可能な各種要素を含む。一実施例では、文書サーバ１０２は、文書サーバが通信しかつアクセスを有する１台以上のコンピュータ上に物理的に位置するディレクトリおよびファイルを有するウェブサーバである。この実施例では、ユーザＡのディレクトリは、例えば文書サーバ１０２上でディレクトリとしてマッピングされる１台以上のマシン上に存在しうる。

【００２０】

文書サーバ１０２は、サーバスクリプト１２２（アクティブサーバページ（ＡＳＰ）等）１２２、トークンデータベース１２４、文書データベース１２６、および認可ユーザデータベース１２８の各要素を含む。サーバスクリプト１２２は、ユーザデバイス１０６または１０８等のクライアントからのｈｔｔｐｓリクエストに応じて作動するスクリプトである。各スクリプトは、クライアントマシンまたはサーバマシン上で作動して希望の動作を

実行できる。文書データベース１２６は、私設ネットワーク１１４の登録ユーザにのみアクセス可能な文書または文書サービス（ここではこれらをまとめてコンテンツと称する）を保存する。

【００２１】

トークンデータベース１２４は、私設ネットワーク１１４の登録ユーザに発行されるトークン関連の情報を記録する。以下に詳述するが、これらトークンは様々な形式をとりうる。形式に応じて、トークンデータベースに記録される発行済みトークン、例えばトークン１２５は、トークンＩＤ（識別子）、ユーザ名、文書またはサービスパス、アクセス権、および監査情報と関連付けることができる。文書またはサービスパスは、認証されたユーザが文書データベース１２６中の文書またはサービスにアクセスできる場所である。監査情報は、トークン発行時刻、トークンの有効期間、およびトークンの有効性（無効にされたかどうか等）、およびトークンの使用方法（トークンがアクセスされたかどうか、何度アクセスされたか等）などを特定する。アクセス権は、トークンをどのように使用できるか、アクセスが付与される文書またはサービスのバージョン、およびトークンが委任可能（すなわち譲渡可能）かどうかなどの情報を特定する。

【００２２】

次に、図１を参照して一実施形態の概要を説明する。デバイスＡ１０６を操作するユーザＡは、デバイスＢ１０８を操作するユーザＢに対して、ユーザＡは登録ユーザ（アカウントを持っている等）だがユーザＢは登録ユーザではない私設ネットワーク１１４の、ファイアウォール１１２の向こう側で利用可能な文書またはサービスへのアクセス権を付与したいとする。従って、ユーザＡがゲートウェイ１１０経由で文書サーバ１０２に対して試みるアクセスはどれも認証され、私設ネットワーク１１４のユーザＡの設定（ユーザアカウント、ユーザ特典、ユーザデフォルトディレクトリ等）へ自動的にマッピングされうる。

【００２３】

最初に、ユーザＡはデバイス１０６からゲートウェイ１１０およびプロキシ１１６のファイアウォール１１２を介して文書サーバ１０２との間で第１の安全なセッションを確立し、ユーザＡがアクセス権を有する文書データベース１２６に保存された文書にアクセスする。続いてユーザＡは、ユニークトークンＩＤとしてＵＲＬ（ユニフォーム・リソース・ロケータ）トークンを作成する。一般にＵＲＬは、（ａ）プロトコルフィールド（ｈｔｔｐｓ等）、（ｂ）ホストコンピュータのアドレスフィールド（ＤＮＳ（ドメインネームシステム）内等）、および（ｃ）パスフィールド（すなわちファイル名またはサービスへのパスを特定）の、３つのフィールドからなる。トークンの送り先である少なくともある公開鍵と、該トークンに関連した他の情報（トークン識別子、パス、アクセス権、作成日等）（以下の図３ではシグニチャコンテンツ３０２と称する）とのデジタル署名入り暗号要約（以下の図３ではＵＲＬトークンシグニチャ３１０と称する）が文書サーバ１０２へ送信され、トークンデータベース１２４中でユニークトークンＩＤと関連付けられる。

【００２４】

その後、ＵＲＬトークンがユーザＡからユーザＢに送信され、これによりユーザＢは、たとえ文書サーバがアクセスをリクエストしているユーザＢを認知していなくても、トークンによって特定される文書またはサービスに対して自由にアクセス（すなわち引換え）できる。ＵＲＬトークンは結合遅延（ｌａｔｅ　ｂｉｎｄｉｎｇ）可能であるという利点があり、このため文書またはサービスコンテンツは受信者がコンテンツを希望する時（例えばコンテンツへのＵＲＬリンクが選択された時）に受信者に送信でき、コンテンツ提供者（ユーザＡ等）から特定の受信者（ユーザＢ等）への文書またはサービスに関する情報の送信時に文書のコピーを提供したりサービスに即座にアクセスする必要がない。

【００２５】

ユーザＡおよびユーザＢから文書サーバ１０２へのアクセスは、ｈｔｔｐｓプロトコル（または当事者双方の認証を必要とする他のプロトコル）を用いて行われる。ｈｔｔｐｓプロトコルの一部として、ユーザ－サーバ間でＳＳＬ接続が確立される。また以下に詳述す

るが、文書またはサービスをサーバ上で閲覧するリクエスト、およびトークンを用いて文書またはサービスにアクセスするリクエストは、ｈｔｔｐｓプロトコルを用いてリクエストされるＵＲＬの形式で行われる。

【００２６】

ユーザＢが文書またはサービスに対するリクエストを行うと、文書サーバ１０２はＳＳＬ接続を立ち上げる一環としてユーザＢ１０８を認証し、ユーザＢの公開鍵を文書サーバに認知させる。その後、文書サーバは、ユーザＡの公開鍵を用いてＵＲＬトークンの一部として含まれるトークンＩＤを認証する（ただしユーザＡが認可ユーザデータベース１２８中に存在する等、私設ネットワーク１１４上の認可ユーザである間に限る）。

【００２７】

図２は、私設ネットワーク１１４の認可ユーザであるユーザＡから私設ネットワーク１１４の認可ユーザではないユーザＢに対するＵＲＬトークン発行の一実施形態を示す。まずユーザＡは、Ｍｉｃｒｏｓｏｆｔ（登録商標）インターネットエクスプローラまたはＮｅｔｓｃａｐｅ（登録商標）コミュニケータ等の一般的なブラウザを呼出すＵＲＬを用いて、文書サーバ１０２またはユーザＢデバイス１０８のいずれかと通信する。ユーザデバイスで選択されたＵＲＬは文書サーバ１０２のサーバスクリプト１２２を呼出し、ユーザデバイスまたは文書サーバ上で動作を実行させる。

【００２８】

一実施形態では、例えばユーザＡ１０６が文書サーバ上のファイルまたはサービスのリストをリクエストするＵＲＬを選択した後、２０２でユーザＡ１０６が文書サーバ１０２との間で（ＳＳＬ等を用いて）安全なセッションを確立して通信が開始される。本実施形態では、ユーザＡのブラウザは、ファイアウォール１１２を抜けてゲートウェイ１１０、プロキシサーバ１１６、および最終的には文書サーバ１０２との間で安全なセッションを確立して開始される。ＳＳＬ接続におけるファイアウォール通過の一方法は、１９９７年３月２６日付けでインターネット上のｈｔｔｐ：／／ｗｗｗ．ｗａｔｅｒｓｐｒｉｎｇｓ．ｏｒｇ／ｐｕｂ／ｉｄ／ｄｒａｆｔ－ｌｕｏｔｏｎｅｎ－ｓｓｌ－ｔｕｎｎｅｌｉｎｇ－０．３．ｔｘ上で発行されたＩＥＴＦインターネットドラフト”Ｔｕｎｎｅｌｉｎｇ　ＳＳＬ　Ｔｈｒｏｕｇｈ　ａ　ＷＷＷ　Ｐｒｏｘｙ”に記載されている。ユーザＡ１０６と文書サーバ１０２との間で安全なセッションを開くことにより、デジタル証明書１３２と１２０とが交換される。

【００２９】

安全なセッションが確立され、ユーザＡが文書サーバの登録ユーザであると認証されれば、２０４で文書サーバがファイルまたはサービスのディレクトリリストのリクエストを受信する。例えばＭｉｃｒｏｓｏｆｔ社製のインターネット情報サーバ（ＩＩＳ）を作動中の文書サーバは、登録ユーザを私設ネットワーク１１４のユーザＡのドメインアカウント上に直接マッピングして、ユーザＡがファイアウォール１１２の内側で動作しているかのようなドメイン中のアクセス特典（すなわち権利と制約）をユーザＡに付与する。２０６で送信されたディレクトリリスト（すなわちユーザＡがアクセス権を有する文書またはサービスへのパスの組）を受信すると、ユーザＡはこのディレクトリリストから選択した文書またはサービス用のＵＲＬトークンを作成するスクリプトを呼出す。呼出されたスクリプトは、スクリプトサーバ１２２上に保存されるか、またはユーザデバイス１０６のキャッシュに記録してもよい。

【００３０】

ＵＲＬトークン作成の一環として、２０８で、ユーザＡは文書サーバから受信したパスの組のうちある文書またはサービスのパスを選択する。２１０では、ユーザＢに利用可能にするためにユーザＡが選択した文書またはサービスの選択パスを文書サーバに送信する。選択パスを受信すると、２１２で文書サーバ１０２は、トークンデータベース中に、ユニークトークンＩＤと選択した（１つまたは複数の）文書またはサービスのパスとで新たなエントリを作成する。２１４で、文書サーバは、選択パスを記録したトークンデータベース中のトークンに関連したユニークトークンＩＤを送信する。２１８でＵＲＬトークンに

署名する前に、２１６でユーザＡ１０６はユーザＢからデジタル証明書情報（デジタル証明書１３４等）を受信しておく必要がある。デジタル証明書情報は、少なくともユーザＢの公開鍵を含まなければならない。

【００３１】

ユーザＢの公開鍵をユーザＡが受信すると、ユーザＡはデジタル署名基準（ＤＳＳ）を用いてユーザＢの公開鍵およびその他のコンテンツ（トークンＩＤ等）に署名する。図３はＤＳＳを実施する公知の一方法を示す。図３では、トークンシグニチャ作成器３００が、ユーザＡの秘密鍵３０８を用いてシグニチャコンテンツ３０２用のＵＲＬトークンシグニチャ３１０（すなわちデジタル署名入り暗号の要約）を作成する。トークンシグニチャ作成器は、暗号化ハッシュ関数３０４と署名ボックス３０６とを含む。一方向性（すなわち非可逆性）と耐崩壊性とを有する暗号化ハッシュ関数３０４の一例として、メッセージ入力（シグニチャコンテンツ３０２等）の１６０ビットのハッシュ出力３０５（すなわち暗号の要約またはメッセージの要約）を生成する、安全ハッシュ基準（ＳＨＳ）で定義された改良型安全ハッシュアルゴリズム（ＳＨＡ－１）がある。一実施形態では、署名ボックス３０６がデジタル署名アルゴリズム（ＤＳＡ）の機能を実行する。

【００３２】

一実施形態では、シグニチャコンテンツ３０２は、ユーザＢの公開鍵３１２と、トークンＩＤ３１４（図２の２１４で送信）、文書（またはサービス）パス３１６（図２の２１０で指定）、およびトークン権３１８（２１０でパスとともに指定可能）等のトークンの他の関連情報とを含む。トークン権３１８は、コンテンツ署名前の任意の時にユーザＡによって指定でき、例えば有効期限、文書をキャッシュ可能な回数、またはサービスの使用可能期間を含む。かかるトークン権はまた、トークンを他者に割当て可能かどうか、および文書またはサービスのデジタル著作権に関する課金情報も指定できる。他の実施形態では、シグニチャコンテンツは３０２、ユーザＢの公開鍵３１２とトークンＩＤ３１４のみを含む。

【００３３】

図２を再び参照して、ユーザＡの秘密鍵での署名後、２２０でＵＲＬトークンシグニチャが文書サーバに送信され、２２２でトークンデータベース１２４に記録され、２２４で安全なセッションが終了する。トークンＩＤの受信後、２２６でユーザＡはいつでもＵＲＬトークンをユーザＢに送信でき、２２８でユーザＢにＵＲＬトークンの受信が通知される。ＵＲＬトークンは、ユーザＡまたは文書サーバ１０２のいずれかによって直接または間接的（例えばＩＲリンク、ｅメール、ＳＭＳメッセージング等によって）に、ユーザＢに送信できる。受信後、ユーザＡが指定したアクセスを除去するか、またはユーザＡが文書サーバ１０２の認可ユーザからはずれない限り、ユーザＢは文書サーバ１０２でＵＲＬトークンを自由に引換えられる。

【００３４】

一実施形態では、ユーザＡはユーザＢに対して、以下の一般的な形式でＵＲＬトークンを提供できる。

［Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｐｒｏｔｏｃｏｌ］：／／［Ｇａｔｅｗａｙ　Ａｄｄｒｅｓｓ］／［Ｓｃｒｉｐｔ］／［Ｔｏｋｅｎ　ＩＤ］．

この一般形式の具体例は、

ｈｔｔｐｓ：／／ｘｅｒｏｘ．ｃｏｍ／ｓｃｒｉｐｔｓ／ＶａｌｉｄａｔｅＴｏｋｅｎ．ａｓｐ？／３２４３３９４９２４，

ここで”ＶａｌｉｄａｔｅＴｏｋｅｎ．ａｓｐ？”はサーバスクリプト１２２から実行すべきスクリプトをさし、数字３２４３３９４９２４はユニークトークンＩＤをさす。

【００３５】

文書サーバ１０２が文書トークンを固有（ユニーク）に特定するには不要かもしれないが、文書名またはサービス名等の追加情報をＵＲＬトークンの一部として含めてもよいことを理解されたい。さらに、ＵＲＬトークン中のスクリプトをＵＲＬの一部として明示する必要はなく、ＵＲＬの宛先であるゲートウェイアドレスから示唆できるようにしてもよい

ことを理解されたい。

【００３６】

図４は、発行されたＵＲＬトークンでキャッシングを行う一実施形態を示す。まずユーザＢ１０８は４０２において、例えばＵＲＬトークンをホットリンクとしてクリックするか、デバイス１０８上のブラウザのアドレスバーにローディングして、ＵＲＬトークンのキャッシングを起動する。これにより４０４でブラウザが文書サーバ１０２と安全なセッションの確立を開始し、この結果、証明書１３４と１２０とが交換される。

【００３７】

安全なセッションの確立に続いて、または安全なセッション確立の一環として、４０６でユーザＢはＵＲＬトークンを文書サーバに送信する。ＵＲＬトークンの構成部分は、スクリプト識別子とトークン識別子である。スクリプト識別子はサーバスクリプト１２２からスクリプト（またはプログラム）を呼出すのに使用され、４０８でスクリプトは、ＵＲＬトークンのユニークトークン識別子構成部分に対応するトークンデータベース１２４中のトークンを特定する命令を実行し、かつトークンがまだ有効である（すなわち無効にされていない）ことを保証する。

【００３８】

トークンの特定後、４０９で、トークンを作成したユーザの証明書の有効性が認可ユーザのデータベース１２８に照会して証明される。トークン作成者であるユーザがトークンデータベース中にトークンとともに記録される。トークンの作成者が現在の認可ユーザでない場合は、トークンは削除またはアクセス不能にされ、ユーザＢにＵＲＬトークンが引換え不可であることが通知される。その後４１０で、特定したトークン中の情報を用いて、安全なセッション（ＳＳＬ接続）確立時４０４に入手したユーザＢの公開鍵によってスクリプトがトークンコンテンツを認証する。

【００３９】

もし（ａ）トークンのシグニチャコンテンツが認証可能である、（ｂ）トークンのアクセス権または監査情報が、ユーザＢが引き続きアクセスを有する（アクセスがユーザＡによるものではない、またはアクセス回数もしくは継続時間が超過していない、またはトークン有効期限が過ぎていない等）ことを示す、かつ（ｃ）ユーザＡがまだ文書サーバの認証ユーザであれば、４１２および４１４で文書データベースから１２６からユーザＢに文書が検索されるか、またはサービスが提供される。その後、４１６でユーザによるアクセスおよび／またはユーザに課される課金を反映するように、トークンデータベースのトークン中でアクセス権または監査情報が更新される。４１８で安全なセッションで文書またはサービスを受信したことがユーザＢに通知され、送信が完了すると４２０で安全なセッションは閉じられる。

【００４０】

図５は、図４の４１０で文書またはサービスへのアクセスリクエストが認証される一実施形態を示す。図５には、非可逆的ハッシュ関数３０４（図３に示す）を用いてシグニチャコンテンツ５０４を処理してハッシュ出力５０５（すなわち暗号の要約）を生成するＵＲＬトークン認証器５０２を示す。どの場合も、シグニチャコンテンツ３０２とシグニチャコンテンツ５０４とが組合され、ユーザＢの公開鍵はユーザＢから直接入手され、トークンデータベース１２４の一部としては記録されない。

【００４１】

ハッシュ出力５０５とトークンデータベース中に記録されたＵＲＬトークンシグニチャとがチェッキングボックス５０６にかけられ、ユーザＡの秘密鍵３０８（図３に示す）とキーペアをなすユーザＡの公開鍵５０８を用いて、シグニチャコンテンツ５０４の真正さを証明する。シグニチャコンテンツ５０４がＵＲＬトークンシグニチャ３１０作成に使用したシグニチャコンテンツ３０２（図３に示す）と同一ならば、認証器の出力はｏｋ信号５１０となり、それ以外ならば認証器の出力はｎｏｔ　ｏｋ信号５１２となる。

【００４２】

ＵＲＬトークンは、文書サーバがユーザＢを事前に認知する必要なく、ユーザＢから文書

サーバ上で利用可能な文書またはサービスへの安全なアクセスを確立するアドホックな方法を提供できるという利点がある。またこの関係は、ユーザＢを文書サーバ上または私設ネットワーク１１４の登録ユーザとして事前に登録する必要なく、ユーザＢからの関与なしでシームレスに管理できる。さらに、ＵＲＬトークンは、ある特定の時点で発行された１つの文書または公開されたサービスではなく、時間とともにダイナミックに変化する文書またはサービス（カレンダ、または税金処理サービス等）への継続的アクセス権をユーザＢに与えるという利点をもつ。

【００４３】

当業者であれば、上記で説明した実施形態は、上述と同様または追加の利点を達成しながら、以下に説明する各種方法に変形可能であることが理解できると考える。また、図中に例示する動作シーケンスまたは構成は、本発明を実行しうる多数の可能なシーケンスの１つを表わすものであり、限定的な意味はない。

【００４４】

図２に示す構成に関して、文書サーバ１０２とユーザＡ１０６とは、２１６でユーザＢから証明書情報（デジタル証明書１３４等）を受信する前、および／または２２０でＵＲＬトークンシグニチャを送信する前に、限定動作２０２，２０４，２０６および２２４を実行する際に安全な通信チャネルを開閉するようにしてもよい。その後、ユーザＡ１０６はＵＲＬトークンに署名してユーザＢ１０８へ通信する。この実施形態では、ユニークトークンＩＤは、２０６でディレクトリリストとともに文書サーバから付与されるか、またはユーザＡによって（文書サーバから事前に発行されたある範囲のトークン識別子を用いるなどして）作成される。

【００４５】

その後のある時点において、文書サーバ１０２とユーザＡ１０６との間で別の安全なセッションが確立され、ここでユーザＡは文書サーバにＵＲＬトークンシグニチャとそれに関連したユニークトークン識別子とを送信する。他の実施形態では、ＵＲＬトークンシグニチャは２２６でユーザＢに送信されるＵＲＬトークンの一部に含めてもよい。この場合、ＵＲＬトークンは、他の場合はトークンデータベース１２４中のトークン識別子と関連付けられるよう２２０で送信されうるトークン識別子情報に加えて、発行されたＵＲＬシグニチャ、文書パス、文書権等の情報を含みうる。ユーザＢから受信後、これら情報はシグニチャコンテンツ３０２（図３に示す）および５０４（図５に示す）に追加され、これにより文書サーバがこれら情報をすべて証明できる。

【００４６】

他の一実施形態では、例えばユーザＡはユーザＢに以下の一般形式をもつＵＲＬを提供できる。

［Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｐｒｏｔｏｃｏｌ］：／／［Ｇａｔｅｗａｙ　Ａｄｄｒｅｓｓ］／［Ｓｃｒｉｐｔ］／［Ｓｉｇｎａｔｕｒｅ］／［Ｒｉｇｈｔｓ］／［Ｄｏｃｕｍｅｎｔ　Ｐａｔｈ］／［Ｔｏｋｅｎ　ＩＤ］．

【００４７】

Ｒｉｇｈｔｓフィールドは、（ａ）トークンの有効期限、（ｂ）トークンをキャッシュ可能な回数、（ｃ）文書トークンを他のユーザに渡すこと（すなわち委任）が可能かどうか、（ｄ）課金および価格情報（例えばＣｏｎｔｅｎｔＧｕａｒｄ（登録商標）デジタルライツ言語ＸｒＭＬ２．０等を用いて指定）、（ｅ）アクセス可能なバージョン、（ｆ）利用期限、（ｇ）発行日、等の情報を含みうる。

【００４８】

この実施形態では、トークンシグニチャは文書サーバのトークンデータベースには保存されないため、ユーザＢはトークン引換え時にＵＲＬトークンシグニチャを提示する。ユーザＡがＵＲＬトークンの一部としてＵＲＬトークンシグニチャをユーザＢに与える利点は、（ａ）ユーザＢがＵＲＬトークンシグニチャを文書サーバに提示する能力が与えられるので、ユーザＡが該トークンを実際に発行していないと文書サーバが主張できなくする、（ｂ）ユーザＢがトークンを他のユーザに委任する委任証明書を構成する能力が与えられ

る（かかる権利がユーザＡから付与された場合）、および（ｃ）ユーザＢがユーザＡからの拒絶から保護（すなわち他者がユーザＡ名でトークンを発行したとユーザＡは主張できない）される。

【００４９】

他の実施形態では、上述したように、ＵＲＬトークンシグニチャはトークンデータベースに保存され、従ってＵＲＬトークンの一部として含める必要がない（ただし含まれるかもしれない）。さらに他の実施形態では、ユーザＡはユーザＢの公開鍵のみに署名する（すなわちシグニチャコンテンツ３０２が少なくともユーザＢの公開鍵からなる）。この実施形態では、トークンデータベースは文書トークンの情報（アクセス権、認可ユーザ、文書パス、監査情報等）と、ユーザＢの公開鍵の暗号の要約とを保存する。この実施形態は、トークンデータベースに保存されるものはすべて安全であり、かつ文書サーバとの安全なセッション中にユーザＡによって通信されるユーザＡの真の意図を反映するものと仮定する。

【００５０】

どの実施形態においても、文書サーバは、ユーザＡがトークン作成に使用した全情報（アクセス権等）へのアクセスを有するか、またはユーザＢに文書またはサービスへのアクセス権を付与する前に、該情報を再構成できなければならない。かかる情報はユーザＡがある時点で（例えばトークン登録時に）文書サーバに送信するか、またはトークンのキャッシュ時（すなわち実行または引換え時）にユーザＢが提示しなければならない。ユーザＡがトークン作成時に用いた全情報を文書サーバが再構成できなければならない理由は、ユーザＡのＵＲＬトークンシグニチャ３１０を証明するため、暗号の要約５０５（図５に示す）生成に用いた情報のビット単位の同一コピーを文書サーバが作成する必要があり、これにより該暗号要約生成に用いたシグニチャコンテンツ５０４の一部として含まれるユーザＢの公開鍵およびその他の追加情報（トークン識別子、作成日、アクセス権等）を認証するためである。

【００５１】

さらに、ユーザＡは、ユーザＢに対してはＵＲＬトークンとともに（図２の２２６で示す）、かつ文書サーバに対してはＵＲＬトークンのシグニチャとともに（図２の２２０で示す）、選択した文書またはサービスの内容または内容の一部の署名入りまたは署名なしの暗号の要約（すなわちコンテンツの要約）を与えてもよい。コンテンツの要約を特定する利点は２つあり、第１にコンテンツの要約をユーザＢに与えることにより、ユーザＢが文書サーバから受信する文書またはサービス（図４の４１８で示す）が、ユーザＡからユーザＢへのＵＲＬトークン発行時にユーザＡがユーザＢに受信させたいと意図したものであることを証明できる。

【００５２】

第２に、コンテンツの要約を文書サーバに与えることにより、ユーザＢの文書またはサービスへのアクセスが文書またはサービスの特定の状態（例えば公開前か公開後か）に限定されること、または文書またはサービスへのアクセスがある種の要素（すなわちＵＲＬトークンで参照される文書またはサービスと文書サーバ上の文書コンテンツとを早く、遅く、または選択時に結びつけること）を含むまたは含まないことを、ユーザＡが文書サーバに指定できる。

【００５３】

一実施形態では、コンテンツの要約は、シグニチャコンテンツ３０２（図３に示す）中に明記されるアクセス権情報に含めてもよい。例えば、アクセス権情報には、選択した文書またはサービスを表わすファイルの現在のコンテンツの要約、または文書サーバ上で動作するバージョン制御システムによって維持される、ある特定時間におけるファイルの状態を示すバージョン番号が含まれうる。バージョン番号は、例えば選択文書またはサービスの現在のバージョン、過去のバージョン、または将来のバージョン等を表わすことができる。

【００５４】

さらに他の実施形態では、公開鍵がわかっている受信者に、ＵＲＬトークンを用いた文書およびサービスへの安全なアクセス権をｅメールで配布するように文書サーバを使用してもよい。

【００５５】

さらに他の実施形態では、発行したＵＲＬトークンへのアクセスの監査および取消し（または修正）メカニズムがユーザＡに与えられる。つまり、ユーザＡはブラウザを利用してサーバスクリプト１２２中のスクリプトを用いてトークンデータベース１２４にいつでもアクセスできる。トークンデータベースを閲覧することにより、ユーザＡはどのトークンが引換えられたか、およびトークンが（例えばあるサービスと）引換えられた頻度、最終引換え時刻、トークン引換えの継続時間等の他の監査情報を特定できる。またトークンデータベースの閲覧により、ユーザＡは発行したＵＲＬトークンの取消し、または発行したＵＲＬトークンの有効期限情報のリフレッシュが可能になる。

【００５６】

一実施形態では、ユーザＡおよびユーザＢは、文書サーバとの間で安全なセッションを確立する際に以下の各行為を行う。すなわち（１）ゲートウェイ１１０が選択ポート上のソケットを開いてプロキシ１１６からの接続を待つ、（２）ゲートウェイ１１０が別ポートまたは同一ポート上のソケットを開いて、ユーザデバイスからの接続を待つ、（３）プロキシ１１６がファイアウォール１１２を介して選択ポート上でゲートウェイ１１０に接続する、（４）ゲートウェイ１１０がプロキシのインターネットアドレスが有効であることを証明する、（５）ユーザデバイスが文書サーバ１０２との間でＳＳＬ接続を確立してゲートウェイ１１０に接続する、（６）ゲートウェイ１１０がユーザデバイスから受信したデータをプロキシ１１６に与え、プロキシ１１６は該データを文書サーバ１０２に与える、（７）プロキシ１１６が文書サーバ１０２から受信したデータをゲートウェイ１１０に与え、ゲートウェイ１１０が該データをユーザデバイスに戻す、（８）ユーザデバイスが文書サーバと通信している間、上記の（６）および（７）を繰り返す。

【００５７】

【発明の効果】

以上の説明をまとめると、本発明は、安全性を損なうことなく、ファイアウォールで保護された特定の文書またはサービスへの安全なアドホックアクセスを可能にする。これにより、安全なネットワーク（ドメイン等）の認可ユーザが、安全なネットワークのファイアウォールで保護された認可ユーザにのみ利用可能な特定の指定文書またはサービスを、安全なネットワークの認可ユーザではない第三者との間で（すなわちトランザクションごとのベースで、または発行ごとのベースで）共有できる。文書またはサービスへのアクセスは、トークンデータベースを介して必要に応じて安全なネットワークの文書またはサービスへのアクセス権を付与し、これによりかかるアクセスのモニタを検討するメカニズム、およびかかるアクセスを（例えばオンデマンドで、一定期間後、所定のアクセス回数後、または所定条件に従って）取消すメカニズムを与えることにより、文書サーバおよび認可ユーザによって能動的に管理される。

【００５８】

トークンによって可能となる可動計算装置に関する追加情報は、米国特許第５，８６２，３２１号および第６，１４４，９９７号（発明の名称「電子文書のアクセスおよび配布システムおよび方法（”Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄｆｏｒ Ａｃｃｅｓｓｉｎｇ ａｎｄ Ｄｉｓｔｒｉｂｕｔｉｎｇ Ｅｌｅｃｔｒｏｎｉｃ Ｄｏｃｕｍｅｎｔｓ”）」に記載されている。

【００５９】

得られるコンピュータ読出し可能なプログラムコードを有する１つまたは複数のプログラムは、メモリデバイスまたは送信デバイス等の１つ以上のコンピュータ利用可能な媒体中で実現できる。従って、本明細書では「製造物」および「コンピュータプログラム製品」という用語は、任意のメモリデバイスまたは任意の送信デバイス等のコンピュータ利用可能な媒体上に（永久に、一時的に、または過渡的に）存在するコンピュータプログラムを

包含することを意図する。

【図面の簡単な説明】

【図１】　本発明を実行する動作環境を示す図である。

【図２】　図１に示す私設ネットワークの認証ユーザであるユーザＡから認証ユーザでないユーザＢにＵＲＬトークンを発行する本発明の一実施形態を示す図である。

【図３】　ユーザＡがＵＲＬトークンのデジタル署名を作成する一方法を示す図である。

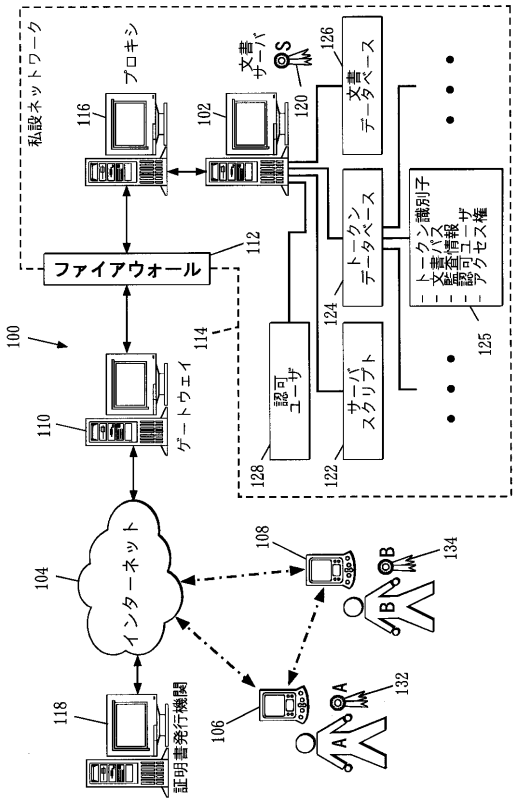
【図４】　発行したＵＲＬトークン中でキャッシングを行う一実施形態を示す図である。

【図５】　文書またはサービスに対するアクセスリクエストを認証する一実施形態を示す図である。

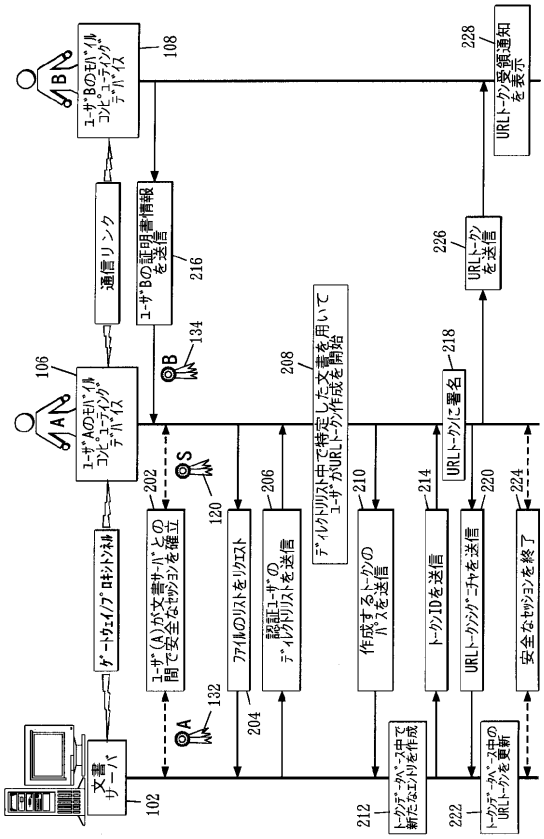
【符号の説明】

１０２　文書サーバ、１０４　インターネット、１０６　第１のユーザ、１０８　第２のユーザ、１１０　ゲートウェイ、１１２　ファイアウォール、１１６プロキシサーバ、１１８　証明書発行機関、１２２　サーバスクリプト、１２４　トークンデータベース、１２５，１２６　文書データベース、１２０，１３２，１３４　デジタル証明書。

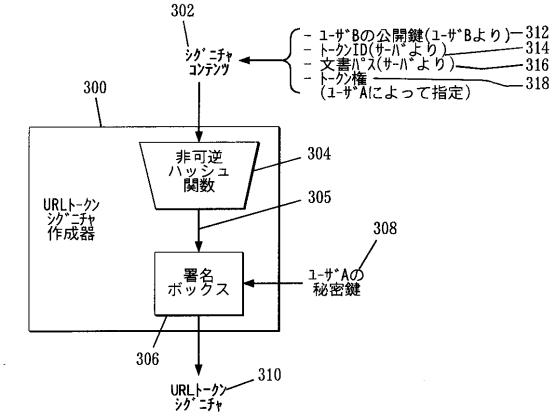
【図１】



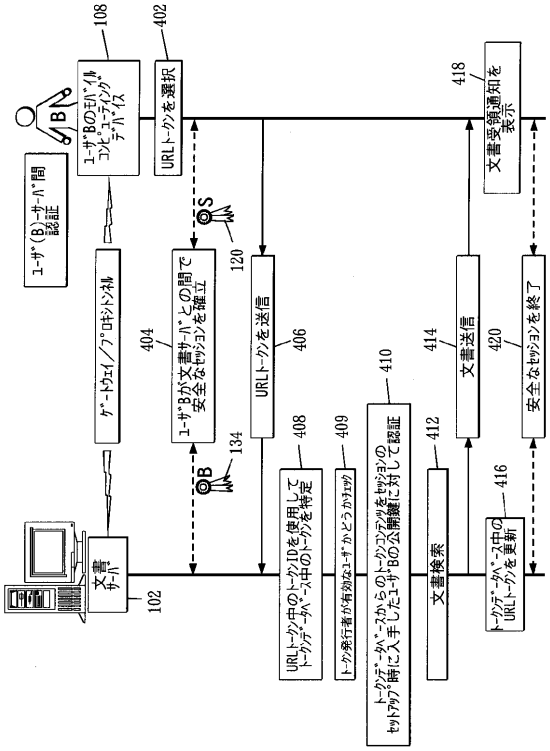
【図２】



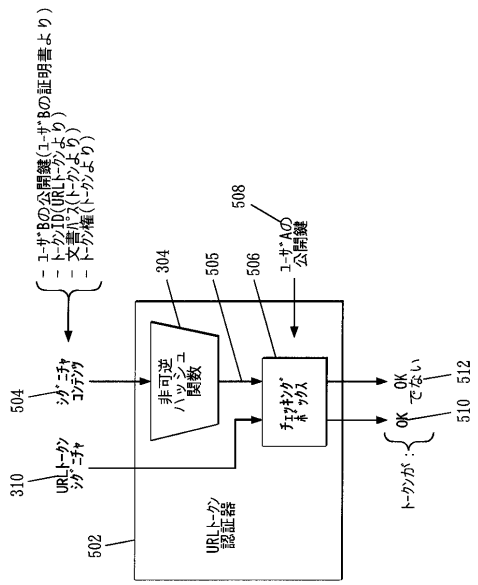
【図３】


302
シグニチャコンテンツ
ユーザBの公開鍵(ユーザBより) 312
トークンID(サーバより) 314
文書パス(サーバより) 316
トークン権(ユーザAによって指定) 318
300
非可逆ハッシュ関数 304
305
URLトークンシグニチャ作成器
署名ボックス
308
ユーザAの秘密鍵
306
URLトークンシグニチャ 310

【図４】


108
402
ユーザBのモバイルコンピューティングデバイス
URLトークンを選択
418
文書受領通知を表示
ユーザ(B)-サーバ間認証
ゲートウェイノードでセッションネゴシエート
404
ユーザBがサーバとの間で安全なセッションを確立
120
URLトークンを送信
406
414
文書送信
420
安全なセッションを終了
134
408
409
410
412
416
文書検索
文書サーバ
102

【図５】


ユーザBの公開鍵(ユーザBの証明書より)
トークンID(URLトークンより)
文書パス(トークンより)
トークン権(トークンより)
508
ユーザAの公開鍵
304
505
506
504
シグニチャコンテンツ
非可逆ハッシュ関数
チェッキングボックス
OK
OKでない
512
510
310
URLトークンシグニチャ
トークンが：
502
URLトークン認証器

フロントページの続き

(72)発明者　エリザベス　ソウトログロウ
イギリス　ハーロウ　チャーチ　ラングレイ　エンスレイ　ガーデンズ　１４２
(72)発明者　ダイアナ　ケイ　スメターズ
アメリカ合衆国　カリフォルニア　バーリンゲイム　ラグナ　アベニュー　９５２

審査官　中里　裕正

(56)参考文献　特開２０００－３１５１７９（ＪＰ，Ａ）
特開２００２－３２３４４（ＪＰ，Ａ）
特開平８－８７３４２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/24
G06F　21/20
H04L　 9/32