社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2006－ＤＳＭ－42／2006－ＱＡＩ－20（９）
2006／7／20

認証チケットを用いた分散認証方式の提案

大久保 敬子　宮城 盛仁　相良 和彦

（株）日立製作所中央研究所 〒185-8601 国分寺市東恋ヶ窪 1-280

E-mail: {keiko-k, miyagi, k-sagara}@crl.hitachi.co.jp

あらまし　ユビキタスネットワーク社会の到来に向けて，複数の認証サーバが連携してユーザ認証を行う分散認証システムを検討した。具体的には，各認証サーバに認証チケット発行・検証機能を持たせ，ユーザ自身が認証情報を認証チケットとして携帯することにより，ユーザの訪問先でのローカルな認証処理を実現する。この際，連携する認証サーバ間で予め公開鍵情報を交換しておき，この公開鍵を用いて認証チケットを検証する。以上により，連携関係にある認証サーバ間であれば，任意の認証サーバが任意のユーザの認証を，他の認証サーバに問い合わせることなくローカルに処理することが可能になり，「いつでも，どこでも，誰でも」というユビキタス性を満たす，大規模な分散認証システムの実現につながる。

キーワード　分散認証システム，ユビキタスネットワーク，認証サーバ

A Proposal of Distributed Authentication Method Using Authentication Ticket

Keiko OHKUBO　Morihito MIYAGI　and　Kazuhiko SAGARA

Hitachi, Ltd., Central Research Laboratory　1-280, Higashi-koigakubo Kokubunji-shi, Tokyo 185-8601, Japan

E-mail: {keiko-k, miyagi, k-sagara}@crl.hitachi.co.jp

Abstract　For a ubiquitous network society, we studied a distributed authentication system in which multiple authentication servers cooperate and perform user authentication. In our proposed system, each authentication server has two functions, issuance and verification of authentication tickets, while each user carries his/her authentication data, issued by his/her local authentication server, using authentication tickets. Each authentication server transmits its public key to each other beforehand, so that these public keys can be used for verifying the authentication tickets issued by other servers. Thereby, any authentication servers can authenticate any users locally, without any inquiry to the other servers. By the proposed system, we can provide a large scale distributed authentication system which satisfies the nature of a ubiquitous network, "Anytime, Anywhere, with Anyone".

Keyword　Distributed Authentication Systems, Ubiquitous Network, Authentication Server

1. はじめに

国家戦略として2001年に策定された「e-Japan戦略」[1]では，日本が5年以内に世界最先端のIT(Information Technology)国家となることを目指し，インフラ・基盤整備に重点を置き，官民産学連携でITの普及に取り組んできた。2003年に策定した「e-Japan戦略II」[2]では，ITの利用活用に目標を移し，利用の促進に向け，サービスの実用化に取り組んできた。更に，これらの政策に続き2004年に策定された「u-Japan政策」[3]は，"ユビキタスネットワーク整備"，"ICT(Information & Communications Technology)の高度化"，"利用環境整備"の3方向で展開され，"価値の創発"を戦略目標とし，2010年の実現を目指している。"利用環境整備"では，ITの普及に伴う不安を解消するために，セキュリティ政策を推進しており，2010年までに国民の80%がICTに安心感を得られる社会にすることを目標として掲げている。

本研究では，セキュリティ強化の重要な要素であるユーザ認証に着目する。ユビキタスネットワーク社会の到来により，人々のネットワークへのアクセスシーンは急速に多様化してきた。これに伴い，ネットワークへのアクセス時のユーザ認証も，ユーザが所属する単一組織の認証ドメイン内での処理から，ユーザの移動を考慮し，複数組織の認証ドメイン間で連携して認証処理を行う方向へと拡張してきている。本研究では，ネットワーク接続時のユーザ認証を地理的，また，ネ

ットワーク構成的に任意の位置から，ユーザにストレスを与えない短い処理時間で行うことを目的とした認証方法を提案する。

2. 従来方式

ユーザ認証を複数の認証ドメインに跨って連携させる場合，従来の方式では，1) ユーザデータベース(以下，ユーザ DB）を統合して一括管理し，一元的にユーザ認証を行う方法（集中管理方式），2) ユーザ DB を認証ドメイン毎に個別に管理し，ユーザ認証は常に対象ユーザの管理元の認証サーバが行う方法（分散管理方式），3) ユーザがアクセスする可能性がある全ての認証ドメインにユーザ情報をコピーしておく方法（ユーザデータ複製方式）がある。以下に，この三つの方法を説明する。

2.1. 集中管理方式

集中管理方式では，図 1に示すように，ユーザ DB を一括して管理する。この例では，ドメイン B に設置された認証サーバ B が全てのユーザのデータを一括管理している。そのため，ドメイン A，C からアクセスするユーザの認証は，認証サーバ B へ問合せて行う。全てのユーザの認証を認証サーバ B が行うため，認証処理の集中が生じる。また，この方法では各ドメインが異なる組織に属する場合には，第三者によってユーザ DB が管理されることになる。このため，各認証ドメインが所属するユーザのデータの第三者への開示を認めない場合，集中管理方式は成立しない。集中管理型の認証方式の例としては，[5]が挙げられる。[5]では，シングルサインオンも同時に実現している。

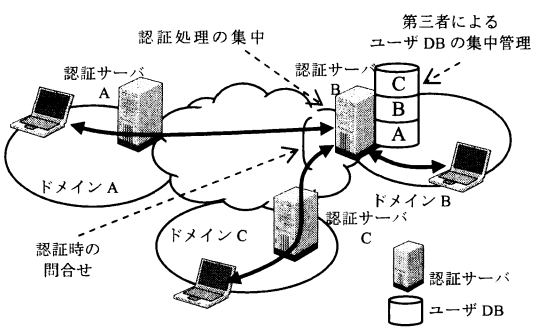

図 1　ユーザ DB 集中管理時の認証処理

2.2. 分散管理方式

分散管理方式では，図 2に示すように各ドメインで，各認証サーバが個別にユーザ DB を管理する。ユーザ認証は，認証対象ユーザの認証データを持つ認証サーバが行う。このため，認証処理の集中は生じない。しかし，ユーザが自分の所属するドメイン以外のドメインからアクセスした場合，認証時には認証サーバ間で問合せが生じる。図 2では，ドメイン A のユーザ a がドメイン B から，ドメイン B のユーザ b がドメイン A から，ドメイン C のユーザ c がドメイン C からアクセスする例を示している。ユーザ a と，ユーザ b の認証処理は，それぞれ認証サーバ A，B が行うため認証サーバ A，B 間で問合せが生じる。以下，他サーバに登録されたユーザをビジターと呼ぶ。また，ユーザからみて，自分が所属するドメインをホームドメイン，ホームドメインの認証サーバをホーム認証サーバと呼ぶ。分散管理方式の例としては[4]が挙げられる。

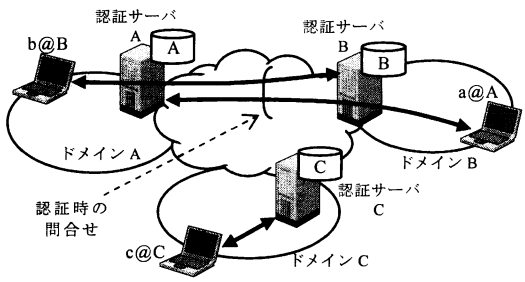

図 2　ユーザ DB 分散管理時の認証処理

2.3. ユーザデータ複製方式

ユーザデータ複製方式では，図 3に示すように各認証ドメインは自ドメインに所属するユーザ以外にも，アクセスを許可するユーザのデータを記録，管理する。ここでは，A",A"'⊂A，B',B"' ⊂B，C',C" ⊂C である。各認証サーバは，予めアクセスしてくる可能性があるユーザのデータを登録しておく。これにより，ユーザデータ登録済みビジターのアクセス時は，ユーザ認証処理において認証サーバ間問合せが不要となる。ただし，登録外の認証ドメインにアクセスしたユーザに関しては，認証サーバ間の問合せが生じる。また本方式では第三者へのユーザデータの開示が必要であると共に，複数の認証ドメインに登録されたユーザデータを，常に最新の状態に保つ必要がある。図 3では，図 2と同様にドメイン A のユーザ a がドメイン B から，ドメイン B のユーザ b がドメイン A から，ドメイン C のユーザ c がドメイン C からアクセスする例を示している。ただし，ユーザ a はドメイン B の A"に登録されているが，ユーザ b はドメイン A に登録されていないとする。

この例では，ユーザ a，c はアクセス先のドメインでローカルに認証されるが，ユーザ b の認証は，認証サーバ B への問合せが必要である。

この例では，必要に応じて選択的にビジターをユーザ DB に登録する例を示したが，全てのユーザのデータを全ての認証ドメインに登録する方法もある。

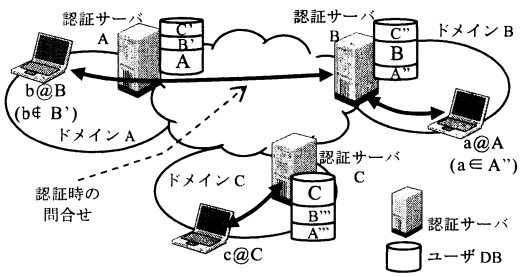

図 3 ユーザデータ複製時の認証処理

3. 認証チケット方式の提案

従来方式では，複数の認証ドメインに跨ったユーザ認証を実現する際に，ユーザ DB の組織別分散管理と，ビジター認証時のサーバ間問合せの省略を両立させることができなかった。本提案では，ユーザ DB の組織別分散管理，認証処理の分散と，ビジター認証時のサーバ間問合せの省略を同時に実現する方法として，ユーザ自身が認証用データを携帯する認証チケット方式を考えた。

3.1. 認証チケット方式の概要

図 4に提案方式の概要を示す。図 4は，ドメイン A に所属するユーザ X が，ドメイン B に移動して認証処理を受ける時の例である。提案方式では公開鍵暗号方式を使用するため，各認証サーバ，ユーザに公開鍵・秘密鍵を設定する。連携する認証サーバ間では予め公開鍵情報のみを交換・共有し，信頼関係を構築する。ユーザは，ホーム認証サーバから認証用の情報を記録した電子証明書（以下，認証チケット）の発行を受ける。その後，移動に伴い訪問先の認証サーバで認証を受ける際は，訪問先認証サーバへ認証チケットを提示する。訪問先認証サーバは，認証チケットの検証をもってユーザ認証とする。これにより，複数組織に跨るユーザ認証の連携において，ユーザデータを各組織で分割管理しつつ，認証時のサーバ間問合せが不要な分散認証を実現する。以下，提案方式の手順を説明する。

① 各認証サーバに公開鍵・秘密鍵を設定し，連携する認証サーバ間で公開鍵情報のみを交換・共有する。
② 各認証サーバはユーザを登録（ID，パスワード，ユーザ公開鍵）する。
③ ユーザ X はホーム認証サーバでログイン認証(ID，パスワード）を行う。
④ ホーム認証サーバはユーザ X へ認証チケットを発行する。
⑤ ドメイン B への移動後，ユーザ X は，訪問先認証サーバ（認証サーバ B）へ，ユーザ認証要求を行う（認証チケットに，要求日時・ユーザ署名を付して提示）。
⑥ 訪問先認証サーバは提示された認証チケットを検証する。
⑦ 訪問先認証サーバはユーザ X へ認証結果を通知する。

認証チケットの構成，及び検証方法は，次節以降で詳細に説明する。

以上の手順により，訪問先認証サーバでのローカルな認証処理が可能になる。

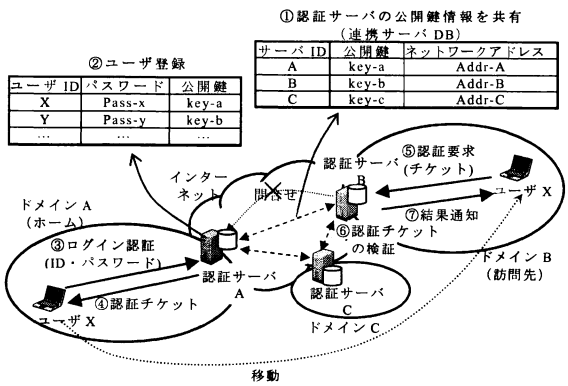

図 4 認証チケット方式の概要

3.2. 認証チケットの構成

認証チケットの構成を図 5に示す。図 5は，ドメイン A のユーザ X がドメイン B へ移動して認証処理を受ける時に用いる認証チケットである。

ユーザ X が認証サーバ A から受信する認証チケット（図 5(I)）は，ユーザ X の ID，公開鍵，属性の他に，認証チケットの有効性を確認する情報として，認証チケットの有効期限，発行元であるホーム認証サーバ名（ここでは認証サーバ A)，ホーム認証サーバの秘密鍵による電子署名を含む。ここでの電子署名は，チケット内の情報のハッシュ値を認証サーバ A の秘密鍵によって暗号化したものである。この電子署名は，認証サーバ A の公開鍵で復号すると，元のハッシュ値に戻る。この電子署名に正しい秘密鍵が使われていない場合は，

認証サーバAの公開鍵で電子署名を復号しても，元のハッシュ値は得られないため，サーバ電子署名の偽造は困難である。

次に，ユーザXがこの認証チケットをサーバBへ提出する際は，要求日時とユーザXの電子署名を追加する。電子署名は，要求日時を含むチケット内の全てのデータのハッシュ値を取り，ユーザXの秘密鍵で暗号化したものである（図 5(II)）。この電子署名は，ユーザXの公開鍵で復号することにより，元のハッシュ値に戻る。ユーザXの電子署名に正しい秘密鍵が使われていない場合は，認証チケット内に記されたユーザXの公開鍵で電子署名を復号しても，元のハッシュ値は得られないため，認証サーバの電子署名と同様に，ユーザ電子署名の偽造も困難である。

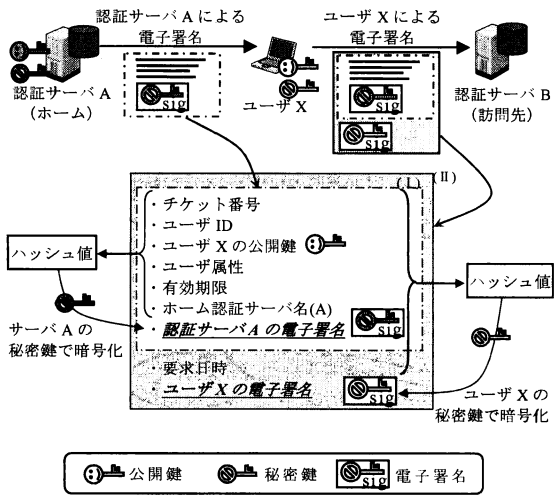

図 5　認証チケットの構成

3.3. 認証チケットの検証

訪問先認証サーバ（ここでは認証サーバB）における認証チケットの検証方法を説明する。認証サーバBは，認証サーバAの電子署名と，ユーザXの電子署名を検証する（図 6）。

認証サーバAの電子署名の検証では，まず，認証チケット（図 6 (I)）内のユーザデータ部分のハッシュ値を計算する。次に，認証サーバAの電子署名を連携サーバDB内に記録してある認証サーバAの公開鍵で復号する。この二つの値が一致する場合，この認証チケットは内容に改竄がなく，認証サーバAの秘密鍵を用いて電子署名がなされた正当な認証チケットである。二つの値が不一致の場合は，認証サーバAの電子署名後に内容が改竄された，又は，認証サーバAの秘密鍵を用いずに不正に電子署名がなされた，偽造の認証チケットである。ホーム認証サーバの電子署名の検証により，これらの認証チケット偽造による成り済ましの防止が可能になる。

同様に，ユーザXの電子署名の検証では，まず，要求日時を含む認証チケット内データのハッシュ値を計算する。次にユーザXの電子署名を認証チケット内に記載されたユーザXの公開鍵で復号する。この二つの値が一致する場合，この認証チケットを提出したユーザは，認証チケット内に記載されたユーザ公開鍵とペアの秘密鍵を持つ正当なユーザである。二つの値が一致しない場合は，認証チケットを提出したユーザは正当なユーザ秘密鍵を持たない不正なユーザである。この検証により，チケット提出者の検証ができ，認証チケット盗用による成り済ましの防止が可能になる。

ホーム認証サーバの電子署名の検証と，ユーザの電子署名の検証の双方に成功した場合のみ，認証成功となる。これにより，訪問先認証サーバでのローカルなユーザ認証が実現する。

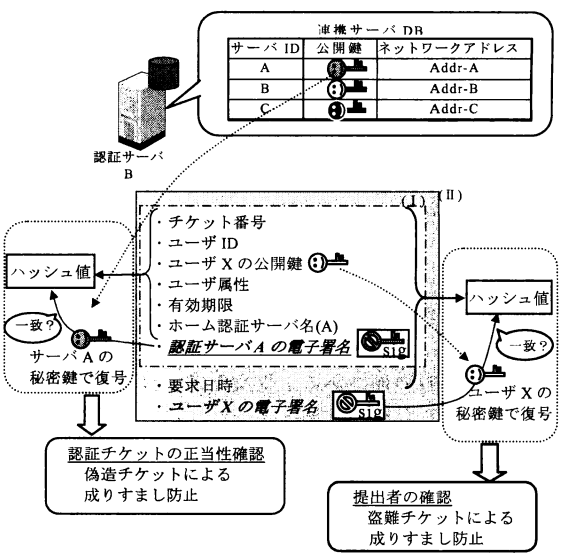

図 6　認証チケットの検証

4. 認証チケット方式の適用例

認証チケット方式の適用例として，企業間連携を考える。ここでは，企業間連携の一例として企業A，B，Cで共同研究を行うために，企業A，Bから企業Cへ人が集まることを考えた（図 7）。

この例では，認証サーバCは，認証チケットを用い

て企業 A，B のユーザの認証処理を行う。事前準備として，認証サーバ C が持つ連携サーバ DB に，認証サーバ A，B の公開鍵を登録する。ここでは，企業 C への集結を前提としており，認証サーバ A，B は連携サーバ DB を持つ必要はない。このように，連携サーバの信頼関係は，必ずしも対称になる必要はない。また，A-C，B-C で認証サーバが連携していても，A-B が連携するとは限らない。

企業 A のユーザ J は，認証チケットを用いて認証サーバ C の認証を受ける。ユーザ J の認証チケットには，属性として企業 C との共同研究の従事者であることが記される。他の情報は，図 5と同様である。認証サーバ A は，ユーザ J の認証処理を行うと，ユーザ J に認証チケットを発行する。ユーザ J が移動し企業 C のネットワークにアクセスする際は，認証チケットに要求日時とユーザ J 自身の電子署名を付加して，認証サーバ C へ提示する。認証サーバ C は，ユーザ J の認証処理として認証チケット内の認証サーバ A の電子署名と，ユーザ J の電子署名を検証し，不正が見つからなければユーザ J に認証成功を通知し，接続を許可する。企業 B のユーザ K に対する認証サーバ C の認証処理も，ユーザ J に対する認証処理と同様であり，認証サーバ B の電子署名と，ユーザ K の電子署名の検証を行う。以上の手順により，認証チケットを用いることにより，認証サーバ C は，企業 A，B のユーザを認証サーバ A，B に問合せを行うことなくローカルに認証することが可能になる。

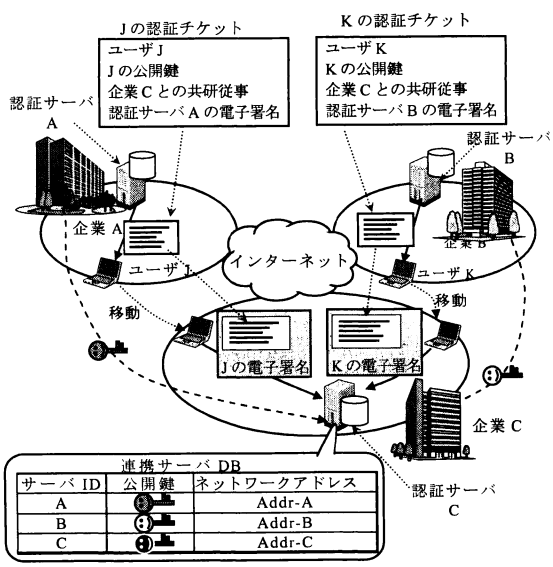

図 7 企業間連携

認証チケット方式は，上記のような企業間連携の他にも，企業間での対称な連携（相互の行き来が可能），企業内での事業所間連携，単位取得などで連携する大学間での連携などへの適用が考えられる。また，連携サーバ DB への登録のみで連携関係が構築されるため，イベントなどの短期間での利用においても利便性は高い。イベント開催前に連携サーバ DB に連携サーバの公開鍵を登録し，イベント終了後には連携サーバ DB の内容を消去することにより，イベント期間のみの連携関係を実現する。

5. 方式比較

2 章で説明した既存の三方式と，提案方式の比較を行う。提案方式ではユーザ DB を分散管理するため，方式の分類上は分散管理方式の認証チケット型とする。また，ユーザデータ複製方式もユーザ DB の管理は基本的に分散であるので，分散管理方式のデータベース複製型と位置づける。

表 1 に各方式の比較を示す。ユーザ DB 管理において，ユーザデータを第三者に開示しないのは，提案方式と，問合せ型の分散管理方式のみである。また，ビジター認証時にサーバ間の問合せが不要なのは，提案方式と，データベース複製型の分散管理方式のみである。以上より，提案方式はユーザ DB の組織毎の個別管理と，ビジター認証時のサーバ間問合せの省略を両立する唯一の方式である。提案方式では，ユーザデータを第三者に開示することなく，認証処理を分散し，ユーザの訪問先でのローカルな認証処理を行う。ただし，ユーザが認証チケットを持っていない場合には，訪問先認証サーバでのローカルな認証処理は不可能であり，ホーム認証サーバへ問合せを行う。

ユーザ DB 変更時の処理は，集中管理方式と問合せ型の分散管理方式では，ユーザデータ管理元で変更処理を行うだけで良いが，ユーザデータ複製型と提案方式では各ドメインでの変更処理後に，連携する認証サーバへの通知が必要になる。提案方式では，例えば，ドメイン A のユーザ Y を認証サーバ A のユーザ DB から削除した時，連携する認証サーバ B，C が発行済みの認証チケットによりユーザ Y を認証してしまうことを防がなければならない。そのために，ユーザ Y の認証チケットが既に無効であることを，連携する各認証サーバへ通知する必要がある。しかし，適用例として考えているような企業間連携，大学間連携などでは，予め認証チケットの有効期限を 3 月末などの異動の時期に設定しておくことにより，有効期限内に無効となる認証チケットの発生を減らし，連携する認証サーバ間での通知量を削減することが可能である。尚，ユーザデータ変更に伴う通知は，認証チケットの無効を通

知するものであり，ユーザデータ自体を通知するものではない。

以上により，認証チケット方式はユビキタス時代の認証方法として利便性が高く，かつ，ユーザデータの秘匿性も高い方式であると考えられる。

表 1 方式比較

	集中管理方式	分散管理方式		
		問合せ型	ユーザデータ複製型	認証チケット型
ユーザDB管理	一括管理 第三者の介在	組織毎 個別管理	組織毎 必要に応じて複製（第三者の介在）	組織毎 個別管理
認証処理	集中	分散	分散	分散
認証時の問合せ	あり	あり	なし*1	なし*2
ユーザDB変更時の処理	DB 管理元で処理	各ドメインで処理	各ドメインで処理 該ユーザを登録している全認証ドメインへ通知	各ドメインで処理 連携ドメインへ通知

*1 DB に登録されていないユーザに対しては，ホーム認証サーバへの問合せによる認証処理を行う。
*2 認証チケットを持たないユーザに対しては，ホーム認証サーバへの問合せによる認証処理を行う。

6. まとめ

ユビキタス時代における分散認証の方法として，認証チケット方式を提案した。認証チケット方式では，認証サーバに認証チケット発行・検証機能を追加し，ユーザ自身が認証情報を認証チケットとして携帯する。これにより，ユーザ DB の分散管理，認証処理の分散を実現しつつ，ビジターの認証においても，訪問先認証サーバにおいて，サーバ間問合せが不要なローカルな認証処理を可能にする。以上より，連携する認証サーバ間では，任意の認証サーバが任意のユーザの認証処理を他サーバに問い合わせることなくローカルに行うことができ，「いつでも，どこでも，誰でも」というユビキタス性を満たす，大規模な分散認証システムの実現へとつながる。

今後の課題として，以下を実施する必要がある。

① 認証チケットによる認証処理時間の定量的評価
② 連携サーバ間で送受信される情報量の評価
③ 規模拡張に向けた検討

今後，上記課題を検討した後，結果をフィードバックし，提案方式の実現に向けて更に詳細な検討を進める。

7. 謝辞

本研究の一部は，平成 18 年度総務省「ユビキタスネットワーク認証・エージェント技術の研究開発」の委託研究による。

文 献

[1] 高度情報通信ネットワーク社会推進戦略本部，“e-Japan 戦略”，http://www.kantei.go.jp/jp/it/network/dai1/pdfs/s5_2.pdf，平成 13 年 1 月（2006 年 5 月調査）

[2] 高度情報通信ネットワーク社会推進戦略本部，“e-Japan 戦略 II”，http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf“，平成 15 年 7 月（2006 年 5 月調査）

[3] 総務省，“u-Japan 政策”，http://www.soumu.go.jp/menu_02/u-japan/index2.htm （2006 年 5 月調査）

[4] J.Kohl, "The Kerberos Network Authentication Service (V5)", IETF, RFC1510, 1993.

[5] Microsoft,"Microsoft Passport Network", http://www.microsoft.com/japan/newsletter/passport.asp（2006 年 5 月調査）