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

2005－DPS－122（27）
2005－CSEC－28（27）
2005／3／22

セキュアサービスプラットフォームにおけるセキュア通信確立モデル

○鍛 忠司　　高田 治　　星野 和義　　藤城 孝宏　　手塚 悟

株式会社　日立製作所

通信に対するセキュリティへの要求が高まるにつれ，ネットワークを伝送される通信データの機密性・完全性の保護を提供する，セキュア通信プロトコルが広く利用されるようになってきている。

既存のセキュア通信プロトコルの多くは，通信データの機密性・完全性を保護した通信を実施するユーザプレーンと，ユーザプレーンを制御するための制御プレーンから構成されている。

本稿では，セキュア通信の制御プレーンを信頼できる第三者が制御し，セキュア通信確立に必要な認証処理等を仲介することにより，セキュア通信を効率よく確立するという，セキュア通信確立のモデルについて述べる。

A Model for Establishing Secure Communication in Secure Service Platform

Tadashi KAJI　Osamu TAKATA　Kazuyoshi HOSHINO　Takahiro FUJISHIRO　Satoru TEZUKA
Hitachi, Ltd.

Secure communication protocols, which provide confidentiality and integrity of communication data, are widely used because of increasing demands of communication security.

Existing secure communication protocols consist of two planes; user plane and control plane. User plane is a function to provide confidentiality and/or integrity of application data, and control plane is a function to control the user plane protocol.

This paper describes a model for establishing secure communication between entities. In this model, a Trusted Third Party controls control plane of secure communication between entities and authenticate the peer entity on behalf of the entities.

１．はじめに

現在，インターネットは電話・放送に次ぐ，第三の情報メディアとして，ビジネスに不可欠な基盤ネットワークとなっている。

その一方で，利用者の個人情報が漏洩したり，身に覚えのない請求が届いたり，といった事件が頻繁に発生し，ネットワークの利用に関する不安が増大している。

この結果，ネットワークや通信に対するセキュリティへの要求が高まり，多くのセキュリティ対策が行われている。通信におけるセキュリティ対策の一例としては，通信の機密性・完全性の保護を提供する，セキュア通信プロトコルが広く利用されるようになってきていることがあげられる。特に，電子商取引では SSL や TLS[3]といったセキュア通信プロトコルが，また，企業の本支社間でデータを交換する場合には IPsec[5][16]といったセキュア通信プロトコルが，多く利用されている。

従来，セキュリティ対策の多くは，一般ユーザやアプリケーションサービス提供者などのネットワーク利用者が自身の PC やサーバ，LAN 等に対策を実施することが一般的であった。

しかし，ネットワーク利用者層の爆発的な拡大や，実施しなければならないセキュリティ対策の増加等から，ネットワーク利用者が十分なセキュリティ対策を実施することは困難になってきている。

今後，誰もがネットワーク社会の利便性を享受するためには，ネットワーク利用者とネットワーク提供者の間でセキュリティ機能を適切に分担することにより，安心して利用できる安全なネットワーク環境を効率よく実現することが望まれている。

例えば，DoS 攻撃を防御する機能を持ったネットワーク基盤技術[13]や企業情報ネットワークを対象として，ネットワークが安全と判断する端末にのみネットワークアクセスを許可するといった技術[14][15]が研究・開発されている。

我々の研究グループでは，ネットワークへのコネクションだけではなく，安全な End-to-end 通信の確立をネットワーク側が代行するネットワーク基盤の研究を行っている[6]~[12]。（このネットワーク基盤を我々は，セキュアサービスプラットフォーム（SSP）と呼んでいる。）

本稿では，SSP が採用しているセキュア通信確立のモデルについて述べる。

以下，2 章で SSP の概要について述べた後，3 章で SSP におけるセキュア通信確立のモデルについて説明し，4 章で TLS や IPsec との比較を行う。

2． SSP 研究開発の概要

SSP は，ネットワーク利用者間の通信を保護するため，ネットワークが信頼できる第三者として振る舞い，ネットワーク利用者の代わりにいくつかのセキュリティ機能を実施するようなネットワーク基盤として研究を行っているものである。

本研究では主に以下に示す 3 つの技術を研究している。

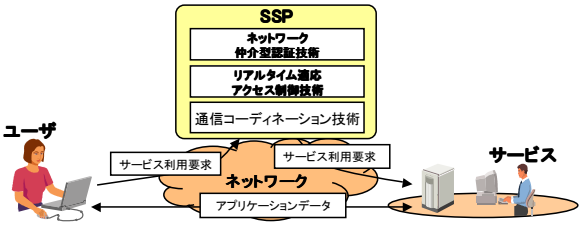

図 2.1 SSP を構成する技術

ネットワーク仲介型認証技術は，煩雑な設定なしに，ユーザが誰であるか，どの IP アドレスを使用しているか，を SSP が認証した上で，ユーザのプライバシーを保護しながらサービスとの接続を確立する技術である。

リアルタイム適応アクセス制御技術は，なりすましや不正アクセスの防止のため，SSP に許可されていない通信や権限のない通信を防止する技術である。

通信コーディネーション技術は，通信に使用するネットワーク回線をサービス・ユーザ側の要求と適合させ，かつ，ユーザ・サービス間の通信セッションの状態を正確に記録・通知する技術である。

SSP では上記の 3 つの技術が有機的に連携することで，ネットワーク利用者の代わりに認証や認可などを実施し，ネットワーク利用者間の安全な通信を実現することを目標としている。

その一つとして，SSP がネットワーク利用者の代わりにセキュア通信を確立したり，制御したりする機能がある。

3． SSP のセキュア通信確立モデル

本章では，SSP がネットワーク利用者の代わりにセキュア通信を確立したり，制御したりする機能のモデル（我々は，仲介型認証モデルと呼んでいる）について述べる。

3.1 階層とプレーン

アプリケーションが利用する通信サービスには様々な機能が含まれている。

OSI 参照モデル[2]が広く知られているが，通信サービスはある特定の機能を提供するプロトコルを階層的に組み合わせられていることが多い。

一方で，あるプロトコル階層の実装の中には，上位層に対してサービスを提供するだけではなく，上位層から制御や管理のためのメッセージ（制御メッセージ）を受けて処理を実行する場合がある。

プレーンとは，上位層とのインタラクションをサービス，制御，管理の機能別に分類・整理したものである[1]。

- ユーザプレーン(user plane)
  上位層へのサービスを実現する機能の集合。
- 制御プレーン(control plane)
  ユーザプレーンでの通信の確立，管理，切断を制御する機能の集合
- 管理プレーン(management plane)
  ユーザプレーンでの通信の確立，管理，切断を管理する機能の集合

なお，プロトコルによっては制御プレーンとユーザプレーンが同じであったり，制御プレーンが存在しなかったりする場合がある。

また，制御プレーンと管理プレーンとは協調して動作することが多いため，以下では，制御プレーンと管理プレーンを纏めて，制御プレーンと呼ぶ。

3.2 仲介型認証モデル

仲介型認証モデルは，信頼できる第三者（TTP）がネットワーク利用者の代わりにセキュア通信を確立・制御するモデルの一つである。

仲介型認証モデルでは，以下の 4 つがプロトコル階層を構成している。（図 3.1）

- Secure communication protocol machine
- Secure signaling protocol machine (SSP machine)
- アプリケーション
- インフラストラクチャ

Secure communication protocol machine はセキュア通信を行うためのオブジェクト（プロトコル機械）であり，アプリケーションは secure communication protocol machine に対してユーザプレーンの上位層にあたる存在である。

一方，制御プレーンに対する上位層には SSP machine という，セキュア通信を制御・管理するためのオブジェクトが存在する。

また，secure communication protocol machine の下位層には IP ネットワークのようなインフラストラクチャが存在する。

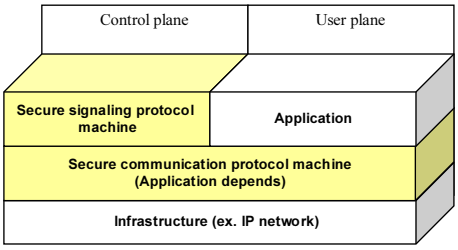

図 3.1 仲介型認証モデルのプロトコル階層

なお，ここでは，セキュア通信におけるユーザプレーンと制御プレーンを以下のように定義する。

- （セキュア通信における）ユーザプレーン

アプリケーションデータの機密性・完全性を保護しながら転送したり，通信相手から受け取ったアプリケーションデータの完全性を確認して上位層に受け渡したりする機能群

・ （セキュア通信における）制御プレーン

ユーザプレーンの通信を確立したり，管理・切断したりする機能群。

なお，ユーザプレーンの通信を確立する場合に，通信相手(Peer)が誰であるか，Peer が通信を行う権利があるか，を確認したり，通信に使用するパラメータを交渉したりする機能も含まれる。

SSP machine は，アプリケーションとは独立したオブジェクトであり，TTP によって制御・管理される。

TTP は SSP machine 間の通信も制御するため，TTP が SSP machine 間の制御チャネル（secure signaling channel）の間に存在し，SSP machine 間の制御メッセージを中継する構成となっている（図 3.2）。

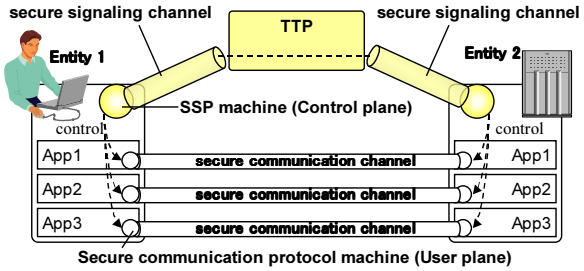

図 3.2 仲介型認証モデル

仲介型認証モデルでの TTP と SSP machine との間の基本的な動作を説明するため，Entity 1 と Entity 2 との間でセキュア通信を確立することを考える。

まず，Entity 1 および Entity 2 の SSP machine は，通信に先立って TTP との間でセキュア通信を確立する。ここで確立したセキュア通信路を使って，各 Entity の SSP machine は TTP および他の Entity の SSP machine と通信を行う。

Entity 1 から Entity 2 に通信確立を要求する場合には，Entity 1 の SSP machine が上で確立したセキュア通信路を使用して，TTP に Entity 2 の SSP machine への通信確立要求を伝送するように依頼する。

Entity 1 から要求を受けた TTP は，Entity 2 との間で確立しているセキュア通信路を使用し，Entity 2 に通信確立要求を転送する。

以下，Entity 1 の SSP machine と Entity 2 の SSP machine は TTP を介して制御メッセージを交換し，Entity 1 と Entity 2 との間のセキュア通信を確立する。

このように，仲介型認証モデルでは，ある SSP machine が他の任意の SSP machine と通信をする場合には，TTP に対して制御メッセージを送信する，あるいは TTP から制御メッセージを受け取る，という動作を行う。

また，TTP は SSP machine 間の制御メッセージを適切に中継する役目を負う。また，TTP が SSP machine の動作を制御する場合には，TTP が制御メッセージを作成して SSP machine に送信する。

さらに，仲介型認証モデルでは，ユーザプレーンを確立するための機能のうち，以下の機能を TTP が SSP machine の代わりに実行する。

(a) Peer が誰であるかの確認（認証）機能

(b) どのような設定で通信を行うのかの交渉（セキュリティパラメータ交渉）機能

(a) Peer 認証機能の代行

一般的なセキュア通信プロトコルでは，通信確立の際に，お互いの身元情報（credential）を交換し，通信相手が誰であるのかを確認している。

一方，仲介型認証モデルでは，SSP machine は Peer の認証処理を行わず，TTP が代行する。

すなわち，SSP machine は，TTP が正しい Peer に通信要求を伝送することを信頼し，通信確立の際に，自分自身の身元情報を提示したり，Peer を認証したり，といった処理を省略する。

上のような Peer 認証の代行を実現するため，各 SSP machine が TTP との間でセキュア通信路を確立する場合には，TTP から認証を受けておく。

また，TTP は複数の SSP machine とのセキュア通信路を維持し，ある SSP machine への制御メッセージを受信した場合には，上の認証結果送信先を識別する。（なお，仲介型認証モデルでは TTP に成りすますことができれば，すべての通信を乗っ取ることができるため，各 SSP machine は TTP との間でセキュア通信路を確立する場合に TTP を認証する。）

(b) セキュリティパラメータ交渉機能の代行

一般的なセキュア通信プロトコルでは，通信確立の際に，お互いに使用可能なすべての暗号アルゴリズムやハッシュアルゴリズムのリストを交換し，ユーザプレーンで使用するアルゴリズムと，そのパラメータを決定し，共有している。

上で述べた処理は保護されていない通信によって行われるため，パラメータの決定には公開鍵暗号や Diffie-Hellman 法などを使う必要がある。

一方，仲介型認証モデルでは，TTP がユーザプレーンで使用するアルゴリズムと，そのパラメータを決定する。

具体的には，TTP が Entity との間でセキュア通信を確立した際に，使用可能な暗号アルゴリズムやハッシュアルゴリズム等の情報を収集しておく。

次に，TTP が Entity 1 の SSP machine から Entity 2 の SSP machine への通信要求を受けた場合には，TTP は Entity 1 が使用可能なアルゴリズムと Entity 2 が使用可能なアルゴリズムとを比較し，もっとも安全と考えられるアルゴリズムとパラメータを決定する。

決定したアルゴリズムとパラメータは TTP が Entity 1 と Entity 2 に配布し，共有する。

このように，セキュリティパラメータを TTP が決定して配布することによって，アルゴリズムのリストを送ったり，公開鍵暗号や Diffie-Hellman 法を使用したりする場合に比べて Entity の負荷を軽減できる。

4. SSP のセキュア通信確立モデルの特長

セキュア通信の確立において，認証処理はユーザからの入力を受け付ける必要があったり，公開鍵暗号などの処理が必要であったりするため，大きな負荷となる。

そこで，本章では，TLS，IPsec，SSP のそれぞれのセキュア通信確立モデルを制御プレーンの数や各 Entity に必要とされる認証処理の回数の観点から比較する。

以下，n 個の Entity が m 種類のアプリケーションを使用し，各アプリケーションがセキュア通信をメッシュ状に確立するような場合について検討する。

(1) TLS の場合

TLS は，以下に示す，複数のサブプロトコルによって構成されている。

- Record Protocol
- Application Data Protocol
- Handshake Protocol
- Change Cipher Spec Protocol
- Alert Protocol

ここで，Handshake Protocol と Change Cipher Spec Protocol，Alert Protocol は，セキュリティパラメータの交渉や使用開始を宣言することによって，Record Protocol の動作を制御している。すなわち，これらのプロトコルは，制御プレーンに属するプロトコルであると考えられる。

Record Protocol は，アプリケーションデータの暗号化や完全性の確認などを行うプロトコルであり，ユーザプレーンに属すると考えられる。

なお，TLS では上で述べた 5 つのサブプロトコルが 1 対となっており，あるアプリケーションで TLS 通信を行う場合，そのアプリケーションが制御プレーン（およびユーザプレーン）を管理・制御している。言い換えると，m 個のアプリケーションでは，それぞれが制御プレーン（およびユーザプレーン）を制御する。

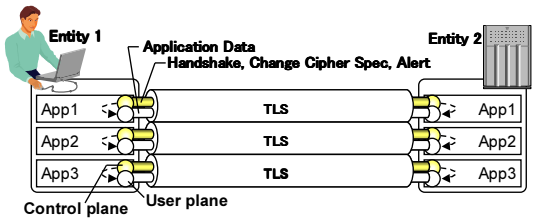

図 3.3 TLS のモデル

あるアプリケーションが TLS を確立する場合には，Peer 毎に認証処理が必要となる。

そこで，m 個のアプリケーションがそれぞれ n-1 個の Peer と TLS を確立する場合に必要な認証処理の回数は，

$$m(n-1)$$

である。

また， n 個の Entity それぞれで同じ数の認証処理が必要となるため，システム全体で必要となる認証処理の回数は，

$$mn(n-1)$$

となる。

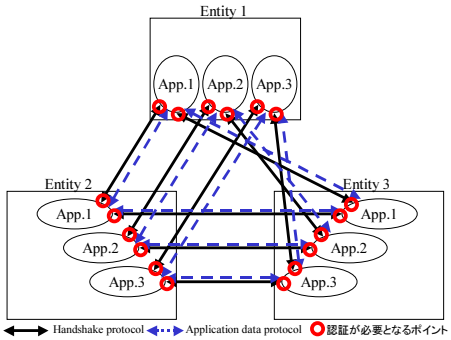

図 5.1 TLS で認証が必要となるポイント

(2) IPsec の場合

IPsec は，Entity 間で共有した SA（セキュリティアソシエーション）に基づいて IP パケットを暗号化したり，認証（メッセージ認証）したりするプロトコルである。

IPsec は，基本的には上位層のアプリケーションデータを暗号化して伝送するための機能しか持たないため，ユーザプレーンに属すると考えられる。

SA を共有する方式には，事前にオフラインで共有する方式（事前共有方式）と，オンラインで共有する方式がある。

IKE[4]は，オンラインで SA を共有することを主な目的として IETF で開発・標準化されたプロトコルであり，IPsec の制御プレーンのプロトコルであると考えられる。

IPsec と IKE は独立したプロトコルであり，ある Entity において IKE を処理するオブジェクト（仮に IKE オブジェクトと呼ぶ）はアプリケーションに依存せず，1 つだけ存在すればよい。

したがって，IPsec を処理するオブジェクトがアプリケーション毎に m 個存在したとしても，1 つの IKE オブジェクトで制御することができる。

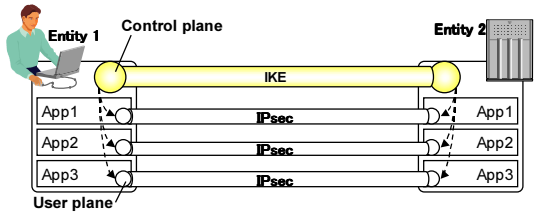

図 3.5 IPsec(+IKE)のモデル

ただし，IKE では，n-1 個の Peer 側の IKE オブジェクトと通信するためには，各 Peer 側の IKE オブジェクト毎に 1 つ，合計 n-1 個の IKE 通信が必要になる。

1 回の IKE 通信につき，1 回の Peer 認証が行われるため，1 つの Entity で必要となる認証処理の回数は，

n-1

となる。

n 個の Entity それぞれで同じ数の認証処理が必要となるため，システム全体では，

n(n-1)

の認証処理が必要となる。

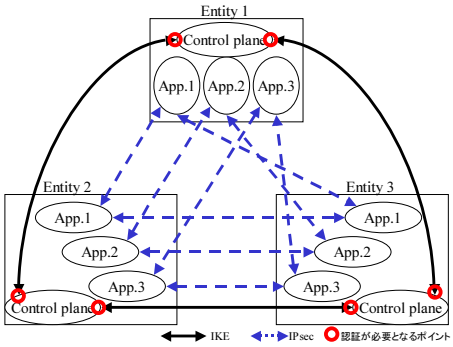

図 5.2 IPsec(+IKE)で認証が必要となるポイント

(3) SSP の場合

SSP でも，IPsec(+IKE)の場合と同様に，アプリケーションとは独立したオブジェクト（SSP machine）が存在し，制御プレーンを管理・制御している。

しかし，IPsec(+IKE)とは異なり，仲介型認証モデルでは，ある SSP machine は TTP とのセキュア通信路を維持しておき，他の任意の SSP machine と通信をする場合には， TTP に対して制御メッセージを送信する，あるいは TTP から制御メッセージを受け取る，という動作を行う。

このため，仲介型認証モデルでは， 1 つの SSP machine で m 個のアプリケーションの secure communication protocol machine が制御できるだけでなく，n-1 個の SSP machine と通信するための制御チャネルも 1 つで済む。

すなわち，SSP machine は TTP との間でセキュア通信を確立する場合にのみ（TTP への成りすましを防止するために）認証処理が必要となる。

したがって，SSP の場合には， 1 つの Entity で必要とされる認証処理は

1

である。

ただし，SSP では，TTP が各 Entity の SSP machine を認証する必要がある。すなわち，TTP において n 回の認証処理が必要となる。

したがって，システム全体としては，n 個の Entity で 1 回の認証処理と，TTP で n 回の認証処理が必要，すなわち，

2n

の認証処理が必要となる。

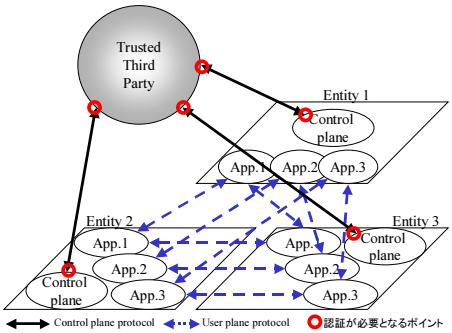

図 5.3 SSP で認証が必要となるポイント

表 5.1 各モデルの比較

	TLS	IPsec (+IKE)	SSP
ユーザプレーン数 (1 Entity 毎)	m	m	m
制御プレーンを制御するオブジェクト数 (1 Entity 毎)	m	1	1
認証処理の数 (1 Entity 毎)	m(n-1)	n-1	1
認証処理の数 (総数)	mn(n-1)	n(n-1)	2n

(n…Entity 数，m…1Entity 上のアプリケーション数)

6. まとめ

通信に対するセキュリティの要求が高まるにつれ，ネットワークを伝送される通信データの機密性・完全性の保護は標準的に提供されるべき機能となってきている。

しかし，このセキュリティ機能を標準的に利用される機能とするためには，可用性・利便性のより一層の向上が必要である。

現在研究を行っている SSP では，セキュア通信の制御プレーンを信頼できる第三者が制御し，セキュア通信確立に必要な認証やセキュリティパラメータの交渉を仲介する，仲介型認証モデルを採用した。

仲介型認証モデルでは，n 個の Entity が m 種類のアプリケーションでセキュア通信を確立するような場合でも，1 つの Entity あたりで 1 回の認証処理しか必要としない。また，システム全体でも 2n 回の認証処理しか必要としない。

今後，セキュアサービスプラットフォームのプロトタイプを開発し， TLS や IPsec(+IKE)等との性能比較を実施していく予定である。

なお，仲介型認証モデルは， TTP をだますことができれば，すべての通信で成りすましが可能になるという問題がある。セキュアサービスプラットフォームの開発に当たっては，Entity－TTP 間でセキュア通信路を確立する場合に高信頼に Entity を認証できる方式を採用することが重要な課題である。

また，仲介型認証モデルは，TTP が認証やセキュリティパラメータの交渉を代行するため，TTP にネットワーク利用者の情報が集中する方式でもある。昨今，個人情報の漏洩が社会的問題になっており， TTP での安全な情報管理やネットワーク利用者のプライバシー保護についても解決する必要があると考えている。

参考文献

[1] ITU-T, I.322,“Generic protocol reference model for telecommunication networks,” ITU-T (1999)

[2] ITU-T, X.200,“Open Systems Interconnection - Basic Reference Model: The basic model,” ITU-T (1994)

[3] T. Dierks etc., RFC2246,“The TLS Protocol Version 1.0,” IETF (1999)

[4] S. Kent etc., RFC2409,“The Internet Key Exchange (IKE) ,” IETF (1998)

[5] S. Kent etc., RFC2401,“Security Architecture for the Internet Protocol,” IETF (1998)

[6] 高田他,“セキュアサービスプラットフォームにおける認証モデルの一検討,” 2005 年電気情報通信学会総合大会 (2005)

[7] 細木他,“セキュアサービスプラットフォームでのセキュリティ状態を用いたアクセス制御に関する検討,” 2005 年電気情報通信学会総合大会 (2005)

[8] 永岡他,“セキュアサービスプラットフォームにおけるプライバシー保護アクセス制御手法の検討,” 2005 年電気情報通信学会総合大会 (2005)

[9] 近藤他,“セキュアサービスプラットフォームにおけるサービス利用権限管理の一検討,” 2005 年電気情報通信学会総合大会 (2005)

[10] 渡辺他,“セキュアサービスプラットフォームにおけるプライバシー保護のための ID 管理方式,” 2005 年電気情報通信学会総合大会 (2005)

[11] 新他,“セキュアサービスプラットフォームのためのクライアントの安全性管理,” 2005 年電気情報通信学会総合大会 (2005)

[12] 小倉他,“セキュリティ・ネットワーク経路選択方式の提案,”電気情報通信学会テレコミュニケーションマネジメント研究会 (2005)

[13] D. Adkins etc., “Towards a More Functional and Secure Network Infrastructure,” UCB Technical Report, No. UCB/CSD-03-1242 (2003)

[14] Cisco,“Network Admission Control,” White paper (2004) (http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd800fdd66.shtml)

[15] Microsoft, “Network Access Protection Platform Architecture,” (2004) (http://www.microsoft.com/windowsserver2003/techinfo/overview/naparch.mspx)

[16] 平野他,“IPsec と IKE を用いたユーザアクセス制御の枠組みの提案と WWW サーバへの適用,”情報処理学会論文誌, Vol.44, No.9, pp.2344-2352 (2003)

謝辞

本稿は，総務省から委託を受けた「高度ネットワーク認証基盤技術の研究開発　－認証機能を具備するサービスプラットフォーム技術－」に関するものである。関係各位のご協力に感謝する。