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の研究開発～
R&D of technologies for advanced network authentication - technologies for secure communication platform based on user authentication

研究代表者　高瀬 晶彦　株式会社日立製作所

研究期間　　平成 16 年度～平成 18 年度

【Abstract】

This paper shows the final results of "R&D of technologies for advanced network authentication - technologies for secure communication platform based on user authentication".

The R&D is about the technologies of network security functions concentrated on platform, so that the users need not make security settings on their computer and also for the service provider they can devote themselves to their own business. And the R&D consists of four fundamental technologies, Technologies for Authentication Mediator Network, Technologies for Realtime-adapted Access Control, Technologies for Communication Coordination, and Technologies for Personal Information Protection.

Now,the R&D theme ends the term of 3years(2004-2006) with many benefical and useful results for the security of network platform infrastructure.

This paper also states many intellectual properties ,technical papers, and presentation materials that had come through the R&D theme.

※

1　研究体制

○　**研究代表者**　　高瀬　晶彦（株式会社日立製作所）

○　**研究分担者**　　田中　俊昭†（株式会社 KDDI 研究所†）

木村　和人††（株式会社インターネットイニシアティブ††）

田中　智博†††（NTT コミュニケーションズ株式会社†††）

岩本　真治††††（日本電気株式会社††††）

沼崎　雅雄†††††（富士通株式会社†††††）

中尾　康二††††††（KDDI 株式会社††††††）

○　**研究期間**　　平成 16 年度～平成 18 年度

○　**研究予算**　　総額　1,396 百万円

（内訳）

平成 16 年度	平成 17 年度	平成 18 年度
674 百万円	425 百万円	298 百万円

２　研究課題の目的および意義

ＩＴの利活用を推進するためには、それを支える社会基盤として安心・安全なインターネット利用環境を整備することが不可欠である。電子商取引を始めとする様々な社会・経済活動を安心して行えるようにするため、本人確認の処理等、高度なセキュリティ機能を具備したネットワーク基盤を構築するために必要となる技術の研究開発を集中的に実施することにより、高度ネットワーク認証基盤技術を確立し、インターネットの安全性・信頼性の向上に資する。

これにより、次世代ネットワーク構築における我が国の主導的立場を確立し、日本企業の国際競争力の向上、世界最先端のＩＴ国家実現に大きく寄与する。

具体的には、インターネット上のなりすましを防止し、通信相手の特定を可能とすることにより、安心してネットワークサービスが利用できるネットワーク環境を実現することを目標とし、ユーザ側の複雑な処理を簡易化したり、ネットワーク上のサービスの利用や提供を安全に行うことができる、高度なセキュリティ機能を有するネットワーク基盤構築のための研究開発を行う。

３　研究成果

３．１　ネットワーク仲介型認証技術

本技術は 100 万規模のユーザに適用できることを目標とする。

利用設定や IP アドレスの登録は、ユーザがネットワークにつないだ際に瞬時に行われる必要がある。そこで、サービスプラットフォームが、ユーザのネットワークへの接続を検知してから、ユーザ端末への利用設定に関する情報を送信するまでの処理を 100msec 程度で完了することを目標とする。また、IP アドレスの登録・更新も、ユーザの電子証明書の有効性の検証、IP アドレスと電子証明書の関連付けの登録・更新完了、ユーザへの登録・更新完了通知をユーザ端末との通信を保護しながら 200msec 程度で完了することを目標とする。また、100 万規模のユーザ数に対応するため、毎秒 1,000 件の登録能力を目標とする。(ピーク時に同時にサーにスプラットフォームに IP アドレス登録を行うユーザを全体の 0.1%と仮定)。

（１）IP アドレス管理と仲介型認証技術の研究開発

① ユーザが使用している IP アドレスを管理する技術の確立

IP アドレス管理技術が具備すべき機能を洗い出し、SIP をベースとしたアドレス管理技術の基本設計を行い、IP アドレスを登録する際に電子証明書によってユーザが誰であるのかを認証し、セキュリティパラメータのネゴシエーションなしに高速に動作する SMS プロトコルを開発した。

② ユーザとサービスとの相互認証を仲介する技術の確立

SIP をベースとして採用し、SIP を用いたユーザからサービスへの接続要求に対して、ユーザとサービスそれぞれの認証を行うための通信手順、およびサービスプラットフォームにおける認証技術を検討し、仕様を策定した。ユーザやサービスに相互認証の結果を通知するための SIP の拡張を検討し、通信先の IP アドレスを現在誰が使用しているかを取得するメッセージ（GETAOR メッセージ）を開発した。そして、ユーザとサービスの間の暗号化通信として IPsec を採用し、その SA（Secure Association）を共有するための

SIP の拡張を検討し､INVITE メッセージの SIP のボディ部分に IPsec の SA 情報を XML フォーマットで記載する方式を開発した。

③ IP アドレス管理システム間連携技術の確立

複数のIPアドレス管理システムが存在する環境でのIPアドレス登録・検索等について方式検討を行い、IPアドレス管理システム間連携のための機能仕様を策定し、これに基づきIPアドレス管理システム間で送受すべきデータとそのタイミングについて検討し、連携のインタフェース仕様を策定した。そしてこれを実験システムにて実験を行うことにより、異なるIPアドレス管理システムに登録されているユーザでも、同一のアドレス管理システムに登録されているユーザと同様の手順で、そのユーザが誰であり、どのIPアドレスを使用しているのかが参照できることを確認した。

④ 相互認証の仲介のためのサービスプラットフォーム間連携技術の確立

複数の仲介型認証システムが存在する環境で、接続先を管理している仲介型認証システムの発見、異なる仲介型認証システムに接続しているユーザ・サービス間の相互認証の仲介等について方式検討を行い、仲介型認証システム間連携のための機能仕様を策定し、これに基づき仲介型認証システム間で送受すべきデータとそのタイミングについて検討した。これらを実験システムにて実験することにより、異なる仲介型認証システムを利用しているユーザとサービスとが同一の仲介型認証システムを利用している場合と同様の手順でセキュアセッションが確立できることを確認した。

⑤ IP アドレス管理システムの負荷分散技術の確立

100万規模のユーザが存在する環境で、すべてのユーザが使用しているIPアドレスと電子証明書の対応付けを管理し、IPアドレスの登録・更新を200msec程度で完了するとともに毎秒1,000件の登録能力を実現する、IPアドレス管理システムの負荷分散技術を検討し、仕様を策定した。これに基づいて実験システムにて実験することにより、負荷分散しているIPアドレス管理システムに登録されているユーザでも、単一のIPアドレス管理システムに登録されているユーザと同様の手順で、そのユーザが誰であり、どのIPアドレスを使用しているのかが参照できることを確認した。

⑥ ユーザとサービスとの相互認証を仲介する際の負荷分散技術の確立

100万規模のユーザが存在する環境で、ユーザからの接続要求を受け付けてから200msec以内でユーザとサービスの相互認証を実施した上で接続要求をサービスに転送できる、仲介型認証システムの負荷分散技術を検討し、実験を行うことで負荷分散している仲介型認証システムを利用しているユーザとサービスとが、単一の仲介型認証システムを利用している場合と同様の手順でセキュアセッションを確立できることを確認した。

以上により、100万規模のユーザが存在する環境で、IPアドレスの管理およびユーザとサービスの相互認証をそれぞれ200msec程度で完了する、IPアドレス管理システム・仲介型認証技術を確立した。

（2）サービス対応 ID 生成管理技術の確立

① サービス対応 ID の生成技術の確立

サービス対応 ID の生成に利用される暗号化の鍵の更新についてサービス対応 ID 生成技

術を確立した。

② サービス対応 ID の管理技術の確立

サービス対応 ID の生成に利用される暗号化の鍵の更新に伴う新旧の暗号化鍵の管理に関してアーキテクチャを確立した。この外、サービス対応 ID 生成管理技術の応用として、メール利用者のプライバシを保護する匿名メールアドレスの生成手法を確立した。

③ サービス対応 ID 提供・利用に関する技術の確立

サービス対応 ID を適切に提供し、利用する技術の基礎方式について検討を行い、その基本的な仕様を確立した。

④ サービス対応 ID 生成管理の連携技術の確立

サービスプラットフォーム間での ID 生成のための情報提供･情報取得の手法について検討を行い､サービスプラットフォーム連携におけるサービス対応 ID の生成に関して基本設計を行った。また、サービスプラットフォーム連携によって生成されたサービス対応 ID の管理について検討を行い、基本設計を行った。そして、サービスプラットフォームの連携によって生成されたサービス対応 ID を利用したサービス利用について検討を行い､基本設計を行った。これらをもとに実験システムにより実験することにより、サービス対応 ID 生成管理の連携できることを確認した。

⑤ サービス対応 ID 生成管理技術の高速化と大容量化

①~④で確立した技術をもとに 100 万規模のユーザが存在する環境で、200msec 以下での ID 生成を行うともに､生成された ID を効率よく管理する ID 管理システムを確立した。

（3） クライアント管理技術の確立

① クライアント設定の自動化とモジュールダウンロード技術の確立

サービス利用のために必要な機能およびモジュールを洗い出し、クライアント設定および自動構築システムの設計を行った。さらにプロトタイプ構築により機能検証を行った。

② アプリケーションに通信リソースを提供する技術の確立

通信リソースを独立のモジュールとして設計するために必要となる機能を洗い出し、基本設計を行った。さらにプロトタイプ構築により機能検証を行い、通信リソースの分離による拡張性や再利用性の高さを確認した。

③ ネットワークインタフェースとアプリケーションインタフェースの機能分担

システム設計の基本思想としてネットワークインタフェースとアプリケーションインタフェースに機能を分離し、それぞれに必要な機能を洗い出し、設計した。さらにプロトタイプ構築により機能検証を行い、管理のしやすさを実証した。

④ サービスプラットフォーム・インタフェース・アプリケーションにおける通信の信頼性を検証する技術の確立

モジュール・インタフェース・アプリケーションに関する情報等をサービスプラットフォームがクライアントに提供する際に、サービスプラットフォームが安全な通信路を提供する技術を確立した。またサービスプラットフォームにおいてクライアント情報の一元的な管理を行うことで、通信や認証を実現するモジュールおよび通信相手のもつ機能の正当性を検証する技術を確立した。

⑤ アプリケーションの利用管理に関する技術の確立

アプリケーションが通信を行うための機能はサービスプラットフォームから提供されるが、これらの機能がサービスプラットフォームに対し想定外の動作を行わないよう、サービスプラットフォーム側からアプリケーションの利用制限を動的に行う技術を開発した。また、サービスプラットフォームと連携して情報を取得することにより、クライアントの機能を管理する技術を確立した。

⑥ モビリティを実現する技術の確立

サービスプラットフォームがクライアントの接続環境に応じた通信方法をクライアントに提供するために、サービスプラットフォームにクライアント接続環境とそれに応じた接続方法や設定を登録する技術を確立した。また、サービスプラットフォームがクライアントの接続環境に応じた設定を選択し、クライアントに提供する技術を確立した。

⑦ クライアントプログラムを自動的に更新するービス技術の確立

クライアントで利用されるモジュールが、バージョンアップや不具合の修正等によって更新された場合、サービスプラットフォームからの指示で自動的にクライアントモジュールを更新する技術を確立した。また、ユーザの意思に応じてプログラム更新を行う技術を確立した。

⑧ クライアント管理の高速化・大容量化技術の確立

ユーザが自動構築システムに接続してから、ユーザ端末への利用設定に関する情報を送信するまでの処理を 100msec 程度で完了する技術を確立した。また、100 万規模のユーザが存在する環境での自動構築システムが出王さするための負荷分散技術として、サービスプラットフォームからユーザ端末にソフトウェアを談ロードする際に安価で効率的な配信技術を確立した。

（4）サービスプラットフォームにおける WEB サービス構築・運用技術の確立

サービスプラットフォームの各要素技術が所期の目標通り連携、機能することを、サービス提供者の視点から確認することを目的に、既存オンラインショップをサービスプラットフォーム対応に改修し、動作確認を行い、サービスプラットフォームの有用性を確認した。更に､サービスプラットフォームを利用した Web アプリケーションの新規作成を支援するライブラリ集を開発し、オンラインショップを作成して動作確認を行った。これらの研究開発を通じて､サービスプラットフォームにおける Web アプリケーションの構築･運用技術を確立した。

３．２　リアルタイム適応アクセス制御技術

きめ細かいセキュリティ・サービス上の要求に対応するため、現状の認証システムでは数項目程度である管理・制御項目を 20 以上の項目で実行できるようにする。同時に、100 万規模のユーザに対してストレスなく接続許可を行うため、1 件当り 200msec 程度の応答時間を実現することを目標とする。

さらに、サービス利用権限を認証する際には、2 段階以上に渡って権限の以上が確実に行われ、かつ毎秒 10 件以上処理できることを目標とする。

（1）リアルタイム適応プロファイル管理技術の研究開発

① リアルタイム適応プロファイル管理技術の確立

プロファイル管理システムで扱うプロファイル情報を、その情報の内容と変更性に注目し、「基本プロファイル情報」「拡張プロファイル情報」「サービス登録プロファイル情報」「端末セキュリティ状態情報」という４つのプロファイル情報項目に分類し、その定義と管理方法を策定した。さらに拡張プロファイル情報については、拡張可能な管理が実現できるユーザオペレーション機能についてそのインタフェース仕様を策定した。

プロファイル状態管理システムで管理するプロファイル情報をリアルタイムに更新し、最新で正確な情報を維持する方式について「プロファイル情報項目、端末セキュリティ状態情報をリアルタイムに登録・更新・削除可能な機能」の基本仕様および詳細仕様を設計した。また、外部情報を取得するためのプロトコル、インタフェースを「プロファイル状態管理システム以外で管理する情報を取得するためのインタフェース機能」および「端末セキュリティ状態情報などプロファイル状態管理システムの外部にある情報を取得するためのインタフェース機能」の基本仕様および詳細仕様を設計した。

② ユーザ・サービスに関する状態対応型アクセス制御ポリシー管理技術の確立

アクセス制御ポリシーの要件を整理し、「アクセス制御ポリシー管理機能」、「アクセス制御ポリシー検証機能」、「ユーザ情報開示制御ポリシー管理機能」、「プロファイル情報の属性情報からユーザ情報開示制御ポリシーの開示制御パターンを生成する機能」について、その基本仕様・詳細仕様を設計した。また、アクセス制御ポリシーについてユーザオペレーション機能として、その登録・更新を行うためのユーザインタフェース仕様について策定した。簡易にポリシーを設定できる機能を実現した。

（２）リアルタイム適応プロファイル制御技術の研究開発

① ユーザ・サービスに関する状態対応型アクセス制御技術の確立

ユーザおよびサービスがお互いに、なりすましや不正アクセスが抑制された状態で安全に通信を行うために、ユーザの状態と、サービスのアクセス制御ポリシーを比較し、接続開示の判断を行う技術を確立した。これにより、適切なサービスを利用できるように、ユーザやサービス提供者の設定したポリシーに従い、通信相手のセキュリティ状態にも対応したアクセス制御技術を実現した。

② 複数サービスプラットフォーム間接続時のアクセス制御連携技術の確立

ユーザの状態とサービス提供者が設定したアクセス制御ポリシーを複数のサービスプラットフォームにて比較し、結果としてサービスへの接続／切断、切断理由の提示、他所方法の提供およびユーザ情報の開示を複数のサービスプラットフォームにて実現するリアルタイムアクセス制御技術を確立した。

③ アクセス制御技術の大容量化・高速化

100万人ユーザの利用を想定し、1件あたり200msecを性能目標として各技術を実現する上で最適なモジュール化や処理分散化の技術を確立した。

（３）サービス利用権限の高度な管理・認証技術の研究開発

① サービス利用権限登録管理技術の確立

利用権限のあり方について要件を分析し、統一的に扱うためのめたモデルを整理した。さらに、メタモデルから基本テンプレートを導出し、データモデル（データ構造）を設計

した。

② 利用権限を示すトークンを利用者に発行する技術の確立

発行するトークンフォーマットおよび、そのトークンの真正性を端プするための方式を開発した。利用権限のデータを XML データフォーマットで提供し、利用権限保有者に見読性を提供し、同時にマシンリーダブルなトークンフォーマットとした。さらにこのフォーマットの脅威分析を行い、真正性、原本性を担保するための電子署名暗号化秘術を導入し、トークンフォーマット拡張仕様を策定した。

③ 利用権限の第三者譲渡を可能とする技術の確立

利用者間での利用権限トークンの分割、権限の有効性検証について基本仕様と詳細仕様を設計した。安全な譲渡方式として、信頼モデル、セキュリティモデルのレベルに応じた譲渡プロトコルを策定した。また、利余権限を第三者に譲渡する場合に不正を防止・抑止するための機能を設計した。

④ 利用権限行使時の正当性検証技術の確立

認証サーバに送られたトークンの正当性を検証する方式について技術開発した。権限行使時に権限管理サーバ上で行うトークンの正当性検証のための方式、手順、DB のデータ構造の基本設計を行った。また、譲渡、有効期限切れなどで権限を失ったトークンのサーバ側での管理方式を設計し、保有している権限トークンが有効かどうかを検証する問い合わせプロトコル仕様を策定した。

⑤ 複数サービスプラットフォーム間接続時の権限管理技術の確立

複数のサービスプラットフォーム間で権限管理を行うためにはサービスプラットフォームにまたがってトークンの有効性確認を行うが、これを実現するためのサービスプラットフォーム間の信頼関係の定義とトークンの検証の際にサービスプラットフォーム間で安全に正当性手順を行う手順について方式を策定した。これらを実験により確認することにより複数サービスプラットフォーム間接続時の権限管理技術の確立されたことを確認した。

⑥ 利用権限処理の大容量化・高速化技術の確立

100 万規模のユーザが存在する環境で、平均して、400msec 程度の処理時間で権限判定処理が可能であり、2 段階以上に渡って権限委譲が可能なサービス利用権限管理の大容量化・高速化技術を確立した。

３．３　通信コーディネーション技術

通信属性として 10 項目以上を想定し、ユーザやサービスの要求条件に適合した通信属性の選択を毎秒 100 件処理し、1 件の選択を 1 秒程度の応答時間で実現する。また、正確な通信ログを生成するため、通信セッションの開始や終了を 200msec 程度で検知し、通信記録を生成するとともに、ユーザやサービスに情報を提供することを目標とする。

（1）通信セッションの状態を検知する技術の研究開発

① 通信セッションの状態(開始・終了・切断）を検知する技術の確立

ドメイン内通信およびドメイン間通信において、通信セッションごとの開始、終了時刻や情報を、ユーザやサービスの側で記録し、その通信記録をサービスプラットフォームの側で一元的に管理する技術を確立した。また、100 万規模のユーザが存在する環境で、通信セッションの開始や終了を 200msec 程度の誤差で検知し、正確な通信記録をサービスプ

ラットフォームで生成・管理する技術を確立した。

（2）ネットワークサービス管理技術の研究開発

① サービス提供者が提供するサービスの特徴・状態などを管理する技術の確立

サービスを効果的にカテゴライズし、サービスの特徴・状態を管理するための基本アーキテクチャを確立するとともに、サービスを登録・更新する場合に用いるプロトコルや処理手順の最適化を検討し、サービスの特徴・状態を管理し、利用者からサービスにアクセスする方式を確立した。

② サービス提供者／ユーザ側からの要求事項を管理する技術の確立

ネットワークサービスへの要求事項を管理するための、基本アーキテクチャを確立するとともに、ネットワークサービスを利用するための要求事項を登録・更新する場合に用いるプロトコルや処理手順の最適化を検討し、ネットワークサービスの要求事項を管理し、利用者からサービスにアクセスする際の方式を確立した。

③ 要求事項とネットワークサービスとのマッチングを管理する技術の確立

ネットワークサービスおよびサービス提供者／ユーザ側からの要求事項管理との連携、類推・補完を高速に行いながら最適なマッチングを行うためサービスプラットフォーム内の他機能との連携方式を検討し設計した。これを実験により確認することで本技術の確立を確認した。

④ 要求事項をネットワークサービスにフィードバックし管理する技術の確立

ネットワークサービスを利用する場合に応じた安全・安心に対する要求度に追従できるように、サービス提供者／ユーザ側の両方からのネットワークサービスへの要求事項に基づいて、ネットワークサービスの動作へフィードバックメインする技術を確立した。

⑤ ネットワークサービス管理の複数サービスプラットフォーム連携技術の確立

複数のサービスプラットフォームが連携する場合に、別のプラットフォームに所属するサービス／ユーザ、ネットワークサービスとの連携を行うための技術を確立した。

⑥ ネットワークサービス管理技術の高速化と大規模化

100 万規模のユーザが存在する環境で、サービスの特徴の定義事項を 10 項目以上持つ条件において、1 秒程度の応答時間を実現する、ネットワークサービス管理の高速化・際規模化技術を確立した。

（3）通信状態を適切に伝達するインタフェース技術の研究開発

① ユーザやサービスに現在の通信状態を適切に伝達するインタフェース技術の確立

サービスプラットフォームが各種情報の収集・管理を行い、ユーザやサービスに通信に関する各種情報を理解しやすい形で伝達し、ユーザやサービスが事象への同意や不同意を容易に選択できる環境を提供するインタフェース技術を確立した。

３．４　その他の研究実績

① 個人情報保護技術の確立

ネットワーク仲介型認証技術、リアルタイム適応アクセス制御技術、通信コーディネーション技術と連携する形で、ユーザが利用したサービスから、ユーザのプライバシーが侵害さ

れることのないように個人情報を保護する技術を確立した。

② 標準化活動

・モバイル環境での認証アークテクチャの一モデルとして ITU-T SG17 課題 9 に提案し、採択された（H17/7)。

・SG17 課題 9 で「TTP を利用するセキュア通信の検討」採用された（H17/10)。

・SSP を含んだ詳細提案がファーストドラフト化された。

③ 実証実験の実施

実インターネット環境にサービスプラットフォームを構築し、これまでの研究成果が実インターネット環境で実現できることを検証するための実証実験を行った。その結果、インターネット環境にサービスプラットフォームを実現できる事を確認した。

4 研究成果の更なる展開に向けて

① 本研究開発における成果の製品化

本研究開発における成果を製品化することで、各技術要素ごとに成果の展開・普及を図る。

通信事業者のネットワークに各要素技術が個別に実装されることで、本研究開発の成果が少しずつ提供され、利用者／サービス提供者それぞれにとって安心・安全なネットワークが段階的に構築される。

② 標準化活動

ITU-T、IETF、ISO 等の国際標準化機関において、引き続き標準化活動を行い、海外への本技術の展開を図る。

これまでの活動：ITU-T に提案を実施中

・モバイル環境における認証アーキテクチャの一モデルとして、SG17 課題 9 に提案し、採用済（05/7）

・SG17 課題 9 で「TTP を利用するセキュア通信の検討」が採用済（05/10）

・本研究開発の成果を含んだ詳細提案がファーストドラフト化

③ 本研究開発における成果の事業化

本研究開発の成果は、高度なネットワーク基盤を構築するためのセキュリティに関する基本的な技術であり、通信事業者の構築するネットワークや企業内の自営ネットワーク等に適用することで本研究開発の成果の展開・普及を図る。

これにより、ユーザ側のインターネット利用等において、安心・安全なネットワーク基盤を実現でき、インターネット上の犯罪の抑制、電子商取引機会の増大等が見込まれる。また、利用者にとっては機器操作が容易となるため、デジタルデバイド解消の一助となり、ますますインターネット利用が活発となることが見込まれる。

5 査読付き誌上発表リスト

[1] Tadashi KAJI, Kazuyoshi HOSHINO, Takahiro FUJISHIRO, Osamu TAKATA, Akifumi YATO, Keisuke TAKEUCHI, Satoru TEZUKA, “TLS handshake method based on SIP,” Journal of Information Assurance and Security (投稿中)

6 その他の誌上発表リスト

[1]星野和義他、“総合力で真の価値創造を目指す日立の次世代ネットワークソリューション”、日立評論 Vol.88 6pp10-12（2006 年 6 月 1 日）:

7　口頭発表リスト

[1]鍛忠司、“高度ネットワーク認証基盤技術研究開発のご紹介－安心・安全なネットワーク社会の実現に向けて－”、データ通信協会　電子署名・認証、タイムスタンプ利用増進セミナー（名古屋市）（2006 年 10 月 27 日）

[2] 星野和義、“高度ネットワーク認証基盤技術研究開発のご紹介－安心・安全なネットワーク社会の実現に向けて－”、データ通信協会　電子署名・認証、タイムスタンプ利用増進セミナー（横浜市）（2006 年 12 月 15 日

[3]鍛忠司、“高度ネットワーク認証基盤技術研究開発のご紹介－安心・安全なネットワーク社会の実現に向けて－”、データ通信協会　電子署名・認証、タイムスタンプ利用増進セミナー（大阪市）（2007 年 2 月 26 日）

[4]鍛忠司、“高度ネットワーク認証基盤技術研究開発のご紹介－安心・安全なネットワーク社会の実現に向けて－”、データ通信協会　電子署名・認証、タイムスタンプ利用増進セミナー（広島市）（2007 年 3 月 9 日）

[5]星野和義、“高度ネットワーク認証基盤技術の研究成果と今後の展開”、安心・安全インターネット推進協議会　平成 18 年度シンポジウム（東京）（2007 年 2 月 26 日）

[6] “Secure Service Platform”、第１０回 Hitachi-Eurecom-NiCT シンポジウム（仏ソフィアアンティポリス）（2006 年 11 月 24 日）

[7]星野和義、“高度ネットワーク認証基盤技術の研究開発と今後の展望”、第 67 回テレコム技術セミナー（東京）（2006 年 10 月 12 日）

[8]日立製作所“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[9]インターネットイニシアティブ“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[10]KDDI、KDDI 研究所“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[11]NTT コミュニケーションズ“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[12]日本電気“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[13]富士通“安心・安全なインターネット利用実証実験”、（東京）（2007 年 1 月 15、16、18、19 日）

[14]日立製作所、インターネットイニシアティブ、KDDI 研究所、KDDI、NTT コミュニケーションズ、日本電気、富士通“高度ネットワーク認証基盤技術の研究開発ワークショップ”、（東京）（2007 年 1 月 17 日）

[15] 日立製作所、インターネットイニシアティブ、KDDI 研究所、KDDI、NTT コミュニケーションズ、日本電気、富士通“Secure Service Platform”、NET&COM2007（東京）（2007 年 2 月 7 日～9 日）

[16] 新 麗、井上 隆仁、桃井 康成、藤並 彰、木村 和人、“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”、電子情報通信学会総合大会(大阪府豊中市)(平成 17 年 3 月 22 日)

[17] 木村 和人, 奥山 大輔, 新 麗、“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管理の実装”、電子情報通信学会総合大会(東京都世田谷区)(平成 18 年 3 月 24 日)
[18] 渡辺　龍　窪田　歩　田中　俊昭､“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 年電子情報通信学会総合大会（大阪)、B-7-20、(2005 年 3 月 22 日）
[19] 渡辺　龍　窪田　歩　田中　俊昭､“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を考慮した ID 生成管理方式の実装”、2005 年 5 月 NS 研究会（奈良)、NS2005-28、(2005 年 5 月 26 日）
[20] 渡辺　龍　窪田　歩　田中　俊昭、“シングルサインオン環境におけるハンドル（ID）の効率的な管理手法に関する一検討”、2005 年電子情報通信学会ソサエティ大会（札幌)、BS-3-7、(2005 年 9 月 22 日）
[21] 渡辺　龍　窪田　歩　田中　俊昭、“セキュアサービスプラットフォームにおけるサービス対応 ID 生成管理システムの実装と評価”、2006 年電子情報通信学会総合大会（東京)、B-7-121、(2006 年 3 月 24 日）
[22] 渡辺　龍　窪田　歩　田中　俊昭、“マルチドメイン環境を考慮したセキュアな ID 管理方式の提案と実装”、NS2006-23、 2006 年 5 月 NS 研究会（京都）(2006 年 5 月 18 日）
[23] 渡辺　龍　窪田　歩　田中　俊昭、“マルチドメイン環境におけるプライバシー保護を考慮した ID 生成管理手法の実装と評価”、FIT2006 第 5 回情報科学技術フォーラム（福岡)、M-023、(2006 年 9 月 6 日）
[24] 渡辺　龍　窪田　歩　田中　俊昭、“プライバシ保護を考慮したハンドル ID 管理方式の大規模ネットワークへの適用に関する検討”、2006 年電子情報通信学会ソサエティ大会（石川)、B-7-98、(2006 年 9 月 22 日）
[25] Ryu Watanabe Ayumu Kubota and Toshiaki Tanaka, “Proposal for Efficient ID Management Scheme on TTP based Authentication Service,” 10th International Conference on Communication Technology, (Guillin), (Nov. 29, 2006)
[26] 渡辺　龍　窪田　歩　田中　俊昭。、“マルチドメイン環境下での認証基盤における ID 管理に関する検討”、2007 年電子情報通信学会総合大会（愛知）
[27]細木正司・田中智博・永岡　孝（NTT コミュニケーションズ)、”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 年電子情報通信学会総合大会（大阪）（2005 年 3 月 22 日）
[28]永岡　孝・森田誠至・細木正司（NTT コミュニケーションズ)、”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 年電子情報通信学会総合大会（大阪）(2005 年 3 月 22 日）
[29]永岡　孝・森田誠至・細木正司（NTT コミュニケーションズ)、”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方式”、2006 年電子情報通信学会総合大会（東京）(2006 年 3 月 24 日）
[30]細木正司・田中智博・永岡　孝（NTT コミュニケーションズ)、”セキュアサービスプラットフォームにおけるセキュリティ状態を用いたアクセス制御方式”、2006 年電子情報通信学会総合大会（東京）(2006 年 3 月 24 日）
[31] 近藤誠、佐原信幸、青木聡、“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 電子情報通信学会総合大会 B-7-19（2005 年 3 月 21 日～24 日）
[32] 青木聡、佐原信幸、近藤誠、“セキュアサービスプラットフォームの複数連携を考慮したサービス利用権限管理の一検討”、2006 年 電子情報通信学会総合大会 B-7-124（2006 年 3 月 24 日～27 日）

[33]小倉孝夫、鈴木啓文、伊勢田衡平、“セキュリティ・ネットワーク経路選択方式の提案”、電子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（石垣市）（2005.03.11）
[34]小倉孝夫、鈴木啓文、原田浩二、廣木聡憲、“セキュリティ・ネットワーク経路選択方式の性能評価”、電子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（久米島町）（2006.03.17）
[35]小倉孝夫、鈴木啓文、原田浩二、廣木聡憲、“セキュアサービスプラットフォームにおけるサービスコーディネート機能の一検討”、電子情報通信学会総合大会（東京都）（2006.3.24）
[36]小倉孝夫、鈴木啓文、原田浩二、福田健一、“認証を用いたIPアドレス詐称防止方式の提案”、電子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（宮古島市）（2007.03.16）
[37] Tadashi Kaji, Kazuyoshi HOSHINO, Takahiro FUJISHIRO, Osamu TAKATA, Akifumi YATO, Keisuke TAKEUCHI, Satoru TEZUKA, “TLS handshake method based on SIP,” Proceedings of 1st International Workshop on Secure Information Systems SIS’06 (ポーランド ヴィシュラ)（2006.11.9）
[38] 上杉忠興、青島弘和、手塚悟、 “TIPS: Trusted Infrastructure Platform for Services”、 第9回 Hitachi-Eurecom-NiCT シンポジウム(フランス ソフィアアンティポリス)(2005.11.24)
[39] Osamu TAKATA, Itsuki WATANABE, Stephane AMARGER, Peter JONES, "Secure Service Platform demonstration" 9th EU Hitachi Science & Technology Forum (ポーランド ワルシャワ) (2006.5.19-21)

8　出願特許リスト

[1] 星野和義、竹内敬亮、高田治、鍛忠司、藤城孝宏、「データ通信方法およびシステム」、日本、米国、欧州、中国、平成 17 年 12 月 13 日
[2] 星野和義、竹内敬亮、高田治、鍛忠司、藤城孝宏、「データ通信方法およびシステム」、日本、米国、中国、平成 16 年 10 月 26 日
[3] 星野和義、鍛忠司、高田治、藤城孝宏、澤田晃平、「サービスネットワークシステムおよびサーバ装置」、日本、米国、欧州、中国、平成 17 年 5 月 11 日
[4] 竹内敬亮、坏毅、「ネットワーク接続システム」、日本、平成 17 年 6 月 13 日
[5] 渡辺　龍　窪田　歩　田中　俊昭、識別情報生成管理装置およびシステムならびにプログラム、日本、平成 17 年 3 月 7 日
[6] 渡辺　龍　窪田　歩　田中　俊昭、識別情報生成管理装置およびシステムならびにプログラム、日本、平成 17 年 3 月 7 日
[7] 渡辺　龍　窪田　歩　田中　俊昭、識別情報生成管理装置およびシステムならびにプログラム、日本、平成 17 年 9 月 6 日
[8]発明者：エヌ・ティ・ティ・コミュニケーションズ株式会社、発明の名称：ネットワーク接続制御システム、ネットワーク接続制御方法、およびネットワーク接続制御プログラム、申請国：日本、申請年月日：平成 17 年 3 月 24 日
[9] 発明者：エヌ・ティ・ティ・コミュニケーションズ株式会社、発明の名称：情報管理装置、情報管理システム、ネットワークシステム、ユーザ端末、及びこれらのプログラム、申請国：日本、申請年月日：平成 17 年 3 月 28 日
[10]小倉孝夫、伊勢田衡平、鈴木啓文、「セキュア通信システム、および通信経路選択装置」、日本・米国、

平成 16 年 12 月 22 日
[11]鈴木啓文、「認証マッチング方法及び装置」、日本・米国、平成 17 年 2 月 17 日

他２６件（出願後未公開のもの）

９　取得特許リスト

[1] 星野和義、竹内敬亮、高田治、鍛忠司、藤城孝宏、「データ通信方法およびシステム」、平成 16 年 10 月 26 日、平成 18 年 9 月 2 日、P3859667
[2] 星野和義、竹内敬亮、高田治、鍛忠司、藤城孝宏、「データ通信方法およびシステム」、平成 16 年 10 月 26 日、平成 19 年 2 月 9 日、P3914959

１０　国際標準提案リスト

[1]ITU-T SG17、CHN-Doc-03、“Proposal on the discussion items related to COM 17-D 53 and COM 17-D 54”、平成 17 年 7 月 11 日
[2]ITU-T SG17、COM17-D75、 "Proposal on the new study item about secure communication using TTP services"、平成 17 年 9 月 22 日
[3]ITU-T SG17、COM17-D143、”Proposal on the process model of secure communications for X.sap-2 “、平成 17 年 4 月 6 日
[4]ITU-T SG17、CAN-Doc-01、“Modified Proposal on X.sap-2”、平成 18 年 9 月 11 日
[5]ITU-T SG17、COM17-C88、“Proposal on X.sap-2 (Secure communication using TTP services)”、平成 18 年 11 月 27 日

１１　参加国際標準会議リスト

[1]ITU-T SG17、モスクワ、平成 17 年 3 月 30 日～平成 17 年 4 月 8 日
[2]ITU-T SG17 合同ラポータ会合、シンセン、平成 17 年 7 月 11 日～平成 17 年 7 月 15 日
[3]ITU-T SG17、ジュネーブ、平成 17 年 10 月 5 日～平成 17 年 10 月 14 日
[4]ITU-T SG17 WP2 会合、ジュネーブ、平成 18 年 1 月 14 日～平成 18 年 1 月 21 日
[5]ITU-T SG17、済州島、平成 18 年 4 月 18 日～平成 18 年 4 月 29 日
[6]ITU-T SG17 合同ラポータ会合、オタワ、平成 18 年 9 月 11 日～平成 18 年 9 月 15 日
[7]ITU-T SG17、ジュネーブ、平成 18 年 12 月 5 日～平成 18 年 12 月 15 日

１２　受賞リスト

該当なし

１３　報道発表リスト

[1]“「安心・安全なインターネット利用実証実験」開催のご案内”、日立製作所 HP、2006 年 12 月 11 日

[2]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施”、日立製作所 HP、2006 年 12 月 11 日

[3]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施”、インターネットイニシアティブ HP、2006 年 12 月 11 日

[4]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術(Secure Service Platform)を一般公開(6 拠点で 7 社合同の一般消費者向け実証実験を実施)”、KDDI 研究所 HP、2006 年 12 月 12 日

[5] “ネットのセキュリティー　利用者、手間軽く　日立などが共同開発”、日経産業新聞、2006 年 12 月 12 日

[6] “ネット安全対策針術”、日本経済新聞、平成 18 年 12 月 12 日

[7] “日立など 7 社　安心・安全な I ネット実現　来年 1 月 15～19 日　実証実験を一般公開”、電波新聞、平成 18 年 12 月 12 日

[8] “日立、IIJ など 7 社が新技術　ネットの安全向上へ　ユーザ側対策を軽減”、電気新聞、平成 18 年 12 月 12 日

[9] “ネット安全利用の技術を共同開発－日立、KDDI など 6 社”、時事通信、平成 18 年 12 月 12 日

[10] “日立、IIJ など 7 社、ネット側にセキュリティ機能を配置する基盤技術を開発”、CNET Japan、平成 18 年 12 月 11 日

[11] “日立、IIJ など 7 社、ネット側にセキュリティ機能を配置する基盤技術を開発”、ZDNet Japan、平成 18 年 12 月 11 日

[12] “日立、IIJ、KDDI など 7 社、ネットワーク側でセキュリティを確保する技術を開発”、MYCOM ジャーナル、平成 18 年 12 月 11 日

[13] “IIJ など 7 社、総務省委託で安全・安心インターネット環境実現する技術”、INTERNET Watch、平成 18 年 12 月 11 日

[14] “ネットワーク側にセキュリティ機能を持たせた「Secure Service Platform」－7 社が開発”、平成 18 年 12 月 11 日

[15] “日立、IIJ ら 7 社、“Secure Service Platform”の実証実験を一般公開”、ASCII24、平成 18 年 12 月 11 日

[16] “一般消費者向けセキュリティ技術を実証実験”、アットマークアイティ（@IT)、平成 18 年 12 月 11 日

[17] “日立など 7 社、「安心・安全なインターネット環境を実現する技術を開発」”、インターナショナルビジネスタイムズ、平成 18 年 12 月 11 日

[18] “日立など 7 社、“セキュアなネット基盤技術”を一般公開”、ITmedia News、平成 18 年 12 月 11 日

[19] “ネットワーク側に高度な安全機能、日立など 7 社が開発”、NIKKEI NET、平成 18 年 12 月 11 日

[20] “日立など 7 社、安心・安全なインターネット環境を実現する技術「Secure Service Platform」を開発”、日経プレスリリース、平成 18 年 12 月 11 日

[21]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開 6 拠点

で 7 社合同の一般消費者向け実証実験を実施”、KDDI HP、2006 年 12 月 12 日

[22]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開 6 拠点で 7 社合同の一般消費者向け実証実験を実施”、公式ホームページニュースリリース、2006 年 12 月 11 日

[23]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開 6 拠点で 7 社合同の一般消費者向け実証実験を実施”、NEC HP、2006 年 12 月 11 日

[24]“総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開 6 拠点で 7 社合同の一般消費者向け実証実験を実施”、富士通 HP、2006 年 12 月 11 日

１４　ホームページによる情報提供

[1]URL　http://network.hitachi.co.jp/SSP.html

掲載情報の概要　「安心・安全なインターネット利用実証実験」開催のご案内

[2]URL　http://www.hitachi.co.jp/New/cnews/month/2006/12/1211b.html

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

[3]URL　http://www.iij.ad.jp/news/pressrelease/2006/1211.html

掲載情報の概要 Secure Service Platform の概要、今後の展開、実証実験の要領を掲載。

[4]URL　http://www.kddilabs.jp/pr_pdf/2006ssp.pdf

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

[5]URL　http://www.kddi.com/corporate/news_release/2006/1211/index.html

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

[6]URL　http://www.ntt.com/release/2006NEWS/0012/1211.html

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

[7]URL　http://www.nec.co.jp/press/ja/0612/1101.html

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

[8]URL　http://pr.fujitsu.com/jp/news/2006/12/11.html

掲載情報の概要 総務省委託研究で研究開発した安心・安全なインターネット環境を実現する技術を一般公開　6 拠点で 7 社合同の一般消費者向け実証実験を実施

研究開発による成果数

	平成 16 年度	平成 17 年度	平成 18 年
査読付き誌上発表数	0 件（ 0 件）	0 件（ 0 件）	1 件（ 1 件）
その他の誌上発表数	0 件（ 0 件）	1 件（ 0 件）	0 件（ 0 件）
口頭発表数	10 件（ 0 件）	23 件（ 2 件）	25 件（ 4 件）
特許出願数	10 件（ 1 件）	24 件（ 8 件）	30 件（ 20 件）
特許取得数	0 件（ 0 件）	0 件（ 0 件）	2 件（ 0 件）
国際標準提案数	0 件（ 0 件）	1 件（ 1 件）	3 件（ 3 件）
国際標準獲得数	0 件（ 0 件）	0 件（ 0 件）	0 件（ 0 件）
受賞数	0 件（ 0 件）	0 件（ 0 件）	0 件（ 0 件）
報道発表数	0 件（ 0 件）	3 件（ 1 件）	23 件（ 0 件）

	合計	（参考） 提案時目標数
査読付き誌上発表数	1 件（ 1 件）	14 件（ 0 件）
その他の誌上発表数	1 件（ 0 件）	0 件（ 0 件）
口頭発表数	58 件（ 6 件）	41 件（ 0 件）
特許出願数	64 件（ 29 件）	50 件（ 0 件）
特許取得数	2 件（ 0 件）	15 件（ 0 件）
国際標準提案数	4 件（ 4 件）	0 件（ 0 件）
国際標準獲得数	0 件（ 0 件）	0 件（ 0 件）
受賞数	0 件（ 0 件）	0 件（ 0 件）
報道発表数	26 件（ 1 件）	6 件（ 0 件）

注１： （括弧）内は、海外分を再掲。

注２： 「査読付き誌上発表数」には、論文誌や学会誌等、査読のある出版物に掲載された論文等を計上する。学会の大会や研究会、国際会議等の講演資料集、アブストラクト集、ダイジェスト集等、口頭発表のための資料集に掲載された論文等は、下記「口頭発表数」に分類する。

注３： 「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等を計上する。