＜基本計画＞

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～

１．目的

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。

２．政策的位置付け

e-Japan 重点計画－2003 において、『2006 年度までに、インターネット等におけるネットワークセキュリティの飛躍的向上を図るため、（中略）認証技術、（中略）等、情報通信ネットワークの安全性及び信頼性の確保に必要となる総合的な研究開発を実施する』ことが目標として掲げられている。

また、「平成１６年度の科学技術に関する予算、人材等の資源配分の方針」（総合科学技術会議）において、重点化すべき研究開発分野として、ネットワークがすみずみまで行き渡った社会に向けた『「高速・高信頼性情報通信システム」技術』が掲げられている。

さらに、「情報通信ソフト懇談会セキュリティWG」において、ネットワーク自体の安全性・信頼性を向上し、電子商取引の更なる発展を促すためには、アクセスしてきたユーザが確かに本人であり、かつ信頼できる利用であるか識別してから特定のサービスを利用できるようなネットワーク基盤を実現するための技術に関する研究開発を実施すべきと提言されている。

３．目標

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ため、本研究開発においては、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。

4. 研究開発内容

① 概要

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環境の実現のため、ネットワーク側に本人確認機能を具備させる等、共通的に必要となる以下のサービスプラットフォーム技術について研究開発を行う。

② 技術課題および到達目標

ア）ネットワーク仲介型認証技術

（技術課題）

なりすましを防止し、安心してサービスの提供・利用ができるようにするためには、ユーザが多種多様な機器で様々な場所からネットワークにアクセスしているような場合でも、煩雑な設定をすることなく、ユーザが誰であり、どの IP アドレスを使用しているのかを簡単に確認できる必要がある。

そこで、以下の技術の研究開発を実施する。

- ユーザがネットワークに接続したり、ユーザがネットワークからログアウトする等、ユーザの使用している IP アドレスが変更になった瞬間に、ユーザ端末とサービスプラットフォームが通信を行い、電子証明書によってユーザが誰であるのかを確認するとともに、ユーザが現在使用している IP アドレスをユーザの電子証明書と対応付けて登録・管理する技術
- サービス利用のためにユーザがサービスと通信を確立するにあたり、サービスプラットフォームがユーザの個人情報が収集されることを防止しつつ、必要に応じてユーザの情報をサービス提供者に通知する技術
- ユーザ端末をネットワークに接続した瞬間に、サービスプラットフォームとユーザ端末とが連携して、サービスプラットフォームを利用するための設定を行う技術

（到達目標）

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出してから、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、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 1000 件の登録能力を目標とする。（ピーク時に同時にサービ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）。

イ）リアルタイム適応アクセス制御技術

（技術課題）

なりすましや不正アクセスを防止するため、サービスプラットフォーム上での許可や権限のない通信を防止する必要がある。

そこで、以下の技術の研究開発を実施する。

- 状況に応じた柔軟なアクセス制御を行うため、サービス提供側、ユーザ側の利用可能な通信手段・セキュリティ状態をリアルタイムに管理し、サービスやユーザの状態に応じて開示するユーザ情報の制御技術
- ユーザがサービス提供者との接続要求をサービスプラットフォームに行った場合に、ユーザの利用可能な通信手段・セキュリティ状態と、サービス提供者が柔軟に設定可能なアクセス許可ポリシーとを確認し、ユーザがポリシーを満たした場合にのみ接続要求を許可する技術
- ユーザがポリシーを満たしており、サービス利用権限を持っていることを認証する技術

本技術では、サービス利用権限の代行や委譲など、高度な権限管理も実現する

（到達目標）

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、毎秒 1000 件程度の接続許可の判定能力と、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委譲が確実に行われ、かつ毎秒 10 件以上処理できることを目標とする。

ウ）通信コーディネーション技術

（技術課題）

インターネットでは信頼性の異なる様々なネットワーク回線が提供されている。安心してネットワークを利用するためには、実際に通信に使用するネットワーク回線がサービス提供者／ユーザ側の要求と適合することが必要である。また、通信が確かに行われたことを保証するため、ユーザとサービス提供者の間の通信セッションの開始、終了、障害発生、通信属性の変化を正確に記録・通知する必要がある。

そこで、以下の技術の研究開発を実施する。

- 通信セッションの開始や終了をリアルタイムに検知し、作成した通信記録を安全に管理する技術
- ユーザやサービス提供者の要求条件に基づいて、最適な通信属性を選択、利用できるための制御技術
- 通信セッションの開始、終了、障害発生、通信属性の情報をユーザやサービスが理解しやすいインタフェースで提供する技術

（到達目標）

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ことを目標とする。

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。

5. 実施期間

平成16年度から18年度までの3年間

6. その他

応募者は、本研究開発で確立した技術の普及啓発活動を実施すると共に実用に向けて必要と思われる研究開発課題への取組も実施すること。

また、その活動計画・方策について具体的に提案書に記載すること。

その他、本研究開発において実用的な成果を導出するための共同研究体制又は研究協力体制についても提案書[5a]（実施体制説明書）の「3　研究開発体制図」や「6　共同研究契約等について」の中へできるだけ具体的に記載すること。