＜基本計画＞

高度ネットワーク認証基盤に関する研究開発

～オンデマンド VPN 技術～

1．目的

インターネット上のなりすましによる被害が社会問題として顕在化している中で、高度な認証機能を誰もが簡便に利用できる基盤の構築を早期に進めることは、安心・安全な IT 利用環境の整備を通じ、インターネットを通じた社会・経済活動を活性化させることに資する。そのため本研究開発において、ネットワーク自体の安全性・信頼性を向上させる認証機能を有するネットワーク基盤構築技術の確立をおこなう。

またこれにより、e-Japan 重点計画に掲げる高度情報通信ネットワーク社会の基盤を確立するとともに、国際的な標準化活動において優位性を確保し、現在米国を中心とする諸外国に席巻されているインターネット関連の技術・製品において我が国の国際競争力を強化する。合わせて重要インフラたるインターネット上のセキュリティ確保において国産技術の確立を図る。

2．政策的位置付け

e-Japan 重点計画－2003 において重点政策分野の「高度情報通信ネットワークの安全性及び信頼性の確保」における、「情報セキュリティに関する基盤技術の研究開発の推進」として、「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」ことがうたわれており、また、認証技術等、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挙げられている。

「情報通信研究開発の推進について」（総合科学技術会議）において、「ネットワークが隅々まで行き渡った社会における様々な新しい情報通信システムに対応する情報セキュリティ技術」の研究開発が重要であり、「モバイルなどの様々なネットワークに対するセキュリティ技術、ネットワーク側が認証機能を有する安全なサービス・プラットフォームの構築などの高度な認証基盤技術、セキュアチップを搭載した機器と IC カードの連携など」が示されている。

さらに、「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、国家的・社会的課題に対応した研究開発の重点化のひとつである情報通信において、「我が国が先行する領域として、情報家電など多種多様で膨大な機器・端末の相互接続・相互運用や、人間と共存するロボットなども新たな核に、IT利用者の視点に立った応用駆動型技術、及び次世代を制するための基礎技術の研究開発・標準化」を特に強化することが示されている。

3．目標

インターネットにおいて、家庭、モバイル、ホットスポットなどのユーザの利用環境や端末の状況に応じた最適なセキュア通信を実現するためには、インターネット上でセキュアな通信を多地点で実現する仮想専用ネットワーク（VPN）を、複数種類かつユーザの要求に即応して、極力人間の介在なく簡易に実現できる柔軟なネットワークが不可欠である。

特に機密性の高い情報を扱う場合には、厳格な機器の認証に基づくセキュアな通信路の確保、および維持を兼ね備えたネットワークが必要となる。

このようなネットワークを、インターネット上で安全かつ簡単・手軽に実現する方法として、高度な認証機能を持ち IC カードの技術を採用するなど安全に証明書や鍵の管理が可能な機器と、それらを管理するサーバにより構成されるネットワーク基盤技術を確立する。

4. 研究開発内容

① 概要

インターネット上で安心してネットワーク・サービスの利用や提供ができる、安全性・信頼性の向上したネットワークを実現するため、機器および仮想専用ネットワーク（VPN）の管理を行うサーバと、高度な認証機能を持ち IC カードの技術を採用するなど安全に証明書や鍵の管理が可能な端末やルータなどの機器を利用することで、利用者の要求に即応して多地点で機器間の VPN を実現するオンデマンド VPN 構成技術等の研究開発を実施する。

② 技術課題及び到達目標

ア）オンデマンド VPN 構成技術

（技術課題）

オンデマンド VPN を構成するためには、構成機器の管理と構成情報の生成が必要である。

構成機器の管理の方法として、IC カードの技術を採用するなど機器に安全に搭載された電子証明書を階層的に利用することで、機器の登録・認証と、複数のオンデマンド VPN において構成可能な機器の登録・認証を、柔軟かつ安全に実現可能とするオンデマンド VPN 構成機器管理技術の研究開発を行う。

また、構成情報の生成においては、管理された機器により、利用者の要求に応じた、ネットワークやサービス、機器の環境、状況に最適な VPN を構成可能とするとともに、多地点での VPN の構成メンバの入れ替えや端末の移動などにより構成が変化した場合にも、オンデマンド VPN を構成する機器の状態などを管理し、実時間内で継続的に状態変化を把握して、ネットワークが柔軟に対応し、継続して VPN を構成可能とする必要がある。そのため、オンデマンド VPN を構成する機器の接続ポリシーや性能、種類等の構成管理情報を条件とし、VPN の機器構成の変化にも柔軟に対応して、機器間の接続構造を示す VPN 構成情報を生成するオンデマンド VPN 構成情報生成技術の研究開発を行う。

さらに、インターネット上の機器が任意の機器とオンデマンド VPN を構築するためには、機器やオンデマンド VPN 構成を管理している単位が異なる場合においても、構成管理情報を相互に運用することが効率的である。そのため、秘匿性などの条件を満たした上で、

オンデマンド VPN を構成する機器の状態などの構成管理情報を複数の管理サーバ間で相互運用を行う構成管理相互接続技術の研究開発を行う。

（到達目標）

大規模な構成においては、100 万台規模の機器が登録されることが想定される。本研究開発では、100 万台規模の機器管理が可能となるように、オンデマンド VPN を新規に構築する場合、およびオンデマンド VPN を構成している機器の一部の入れ替えにより VPN を再構成する場合に、構成情報を1秒未満で生成できることを目標とする。

さらに、複数の管理サーバ間における VPN 構成管理情報の交換を可能とするため、他の管理サーバからの情報交換の要求に対する応答を1秒以内で実現することを目標とする。

イ）オンデマンド VPN 鍵配送管理技術

（技術課題）

VPN 構成情報に従い、機器に対して、様々なサービスに対応した厳格なセキュリティ確保を可能とする必要がある。そのため、IC カードの技術を採用するなど機器に安全に搭載された電子証明書を、機器の情報登録や、各々のサービスが互いに独立、階層的に利用することで、安全な鍵や構成情報等の配送、ならびに安全な管理を行うオンデマンド VPN 鍵配送管理技術を研究開発する。

また、ルータなどの機器においては、複数の機器とのオンデマンド VPN 接続を構成することが求められる。そのため、多地点・複数機器との接続を実現することを可能とする。

（到達目標）

多地点間でかつオンデマンドに VPN を実現可能とする鍵配送管理技術として、具体的には、3 秒以内で VPN 構築を実現可能とする。

さらに事業所や家庭内の機器が、ルータなどの機器を利用してインターネットと接続され、外部の機器と多地点間で VPN 接続される場合を想定し、VPN を構成する 100 万台規模の機器に対応できるように、各々の接続する VPN に応じた 500 個程度の鍵を管理可能とする。

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

本研究開発で実現する技術に関して、個別企業に特化することなく広く普及・実現するため、普及促進を行う組織との連携をはかること。