

<基本計画>

経路ハイジャックの検知・回復・予防に関する研究開発

1. 目的

インターネットは、ISP、大学、企業等の主体が運営するネットワーク同士が相互に接続したネットワークである。各ネットワークでは、通信経路を確立するための経路情報を保持・交換しているが、不正な経路情報が交換されることにより、インターネットにおける経路情報の誤りによる通信障害(以下「経路ハイジャック」という。)が発生しており、障害の検知・回復にかなりの時間を要しているのが実状である。

このため、経路ハイジャックを検知・回復・予防する技術を確立し、インターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現することを目的とする。

2. 政策的位置付け

「第2期科学技術基本計画」(平成13年3月閣議決定)の「第2章 I. 科学技術の戦略的重点化 2. 国家的・社会的課題に対応した研究開発の重点化 (2)情報通信分野」中の「ネットワーク上であらゆる活動をストレスなく時間と場所を問わず安全に行うことのできるネットワーク高度化技術」に該当する。

「分野別推進戦略」(平成13年9月総合科学技術会議)の「情報通信分野 高速・高信頼情報通信システム (2)重点領域 ウ」中の「利便性、安全性(セキュリティ)・信頼性、…のための技術」に該当する。

「e-Japan 戦略Ⅱ」(平成15年7月IT戦略本部)の「Ⅲ. 新しいIT社会基盤の整備 2. 安全・安心な利用環境の整備」において、「情報システムの脆弱性の低減、コンピュータウイルス対策等の情報セキュリティに関する技術について、民間による技術開発に加え、国においても、先導的基盤的研究開発を推進する。」こととされている。

「u-Japan 政策」(平成16年12月総務省)の「ネットワークの高信頼性確保」において、「脆弱性を克服し、災害やテロ等の非常時にも強いネットワークを実現し、高信頼性を確保するために、セキュアネットの基盤技術の開発を推進する。」こととされている。

「平成18年度の科学技術に関する予算、人材等の資源配分の方針」(平成17年6月総合科学技術会議)の「①重点4分野 (b)情報通信」において、「ネットワークがすみずみまで行き渡り、便利で安全・快適に暮らせるユビキタスネット社会の実現に向けて、(中略)、ITシステムの利便性、信頼性、安全性に資する技術等の研究開発及び実証の推進。」が挙げられている。

「経済財政運営と構造改革に関する基本方針2005」(平成17年6月経済財政諮問会議)において、「IT戦略の推進」のための取組として、「官民における統一的・横断的なセキュリティ

対策を推進する。」、「ネットワーク分野について、2010 年までにユビキタスネット社会を実現するために、「u-Japan 政策」を推進する。」及び「IT を活用した安心・安全への取組を推進する。」こととされている。

「次世代 IP インフラ研究会 第二次報告書 ～「情報セキュリティ政策 2005」の提言～」(平成 17 年 7 月 総務省)において、経路情報の誤りによる ICT 障害について、「障害の検知・回復・予防に関する研究開発」に早急に取り組むべきこととされている。

「ユビキタスネット社会に向けた研究開発の在り方について ～UNS 戦略プログラム～」(平成 17 年 7 月 総務省)の「ユビキタス重要研究開発 3 戦略と 10 のプロジェクト」における「セキュアネットワーク」に該当し、「サイバーテロ、災害等の非常時を含め、いつ何時でも各人にとって必要な通信を確保するため、壊れても自動的に治癒・対処・予防・保証することを可能とする世界最強水準のネットワーク・ライフライン技術を 2010 年までに実現する。」こととされている。

3. 目標

(1) 政策目標

インターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現する。

(2) 研究開発目標

経路ハイジャックを速やかに検知し、自律的に回復し、未然に予防するため、平成 21 年度を目標に次の①～③の技術に関する研究開発を実施し、i)～iii)の目標を実現する技術を確立する。

(技術課題)

① 経路ハイジャックの検知技術

他のネットワークの保有している経路情報を手動ではなく自動的に確認すること等により、経路ハイジャックを速やかに検知することを可能にする技術

② 経路ハイジャックの回復技術

検知の結果を元に、障害の要因と影響の範囲の特定から、経路情報の誤りの回復に至るまでを自律的に行う技術

③ 経路ハイジャックの予防技術

他のネットワークによる不正な経路情報の登録の防止等、経路情報のデータベースの信頼性を向上させ、経路ハイジャックを予防する技術

(目標)

i) 経路ハイジャックの迅速な検知等

ii) 経路ハイジャックからの自律的な回復等

iii) 不正な経路情報登録の防止等による経路情報データベースの信頼性向上等

4. 研究開発内容

①概要

(ア)経路ハイジャックの検知技術

経路ハイジャックを自律的かつリアルタイムに高精度で検知するためには、インターネットの複数箇所で多面的な監視を行い、監視ポイントで得られる膨大な経路情報などを効率的に処理・分析する必要がある。

これを実現するために、エージェントを複数箇所に配備し、エージェント間の連携により自律的かつリアルタイムに経路ハイジャックを検知するエージェント分散型経路監視技術について研究開発を実施する。

(イ)経路ハイジャックの回復技術

検知された経路ハイジャックに対して、その原因である経路不正広告元の特定やその影響度を分析し、経路情報の回復(誤った経路広告を元に戻すこと)を自律的に行う技術とともに、エージェントが配備された箇所では不正経路広告を受信しないなどの不正経路広告元を切り離す技術について研究開発を実施する。

(ウ)経路ハイジャックの予防技術

経路情報の信憑性を確認するIRR(Internet Routing Registry)の安全性、信頼性の向上を可能とする技術の研究開発を実施し、経路ハイジャックを未然に防ぐ現実的な予防技術を確立する。

以上の技術をネットワークノード、運用管理システムに組み込み、実用レベルのネットワークにおける実証実験を行うことにより、実用化を図る。

②技術課題および到達目標

(ア)経路ハイジャックの検知技術

(技術課題)

経路ハイジャックは、国内あるいは国外において、BGP(Border Gateway Protocol)オペレータが間違った(不正な)経路情報を広告するなどにより発生する。しかし、現状では、ISP が自ら利用しているIPアドレス空間と自AS(Autonomous System)番号の組み合わせ(経路情報)を、他ISPによりインターネット内に広告され、自ISPの通信が不通になっても(経路ハイジャックされていても)、自律的には把握できない状況である。また、逆に、自ISPが、他ISPの利用するIPアドレス空間を自IPアドレス空間として、誤ってインターネット内に経路広告することにより、他ISPの通信が不通になっても(経路ハイジャックしてしまっても)、自律的には把握できない状況である。

これらを解決する経路ハイジャック検知技術を確立するため、複数箇所に配置されたエージェントで経路情報を監視し、エージェント間でセキュアな情報連携を行い、経路ハイジャックを検知する、エージェント分散型経路監視技術について研究開発を実施する。

(到達目標)

国内外で発生した経路ハイジャックを数分以内で検知可能とするエージェント分散型経路監視技術を確立する。

(イ) 経路ハイジャックの回復技術

(技術課題)

経路ハイジャックが発生した場合、現状では自律的に診断・回復する技術が無く、不正な経路広告元の特定や誤った経路広告の停止などの回復作業を、人手を介して行っているため、多大な時間を要している。

これらを解決するために、インターネット上の複数箇所に配置したエージェントから得られる情報を元に障害範囲などを分析し、当該箇所に配備されたエージェント間の連携により、自律的に経路ハイジャック状態を回復するとともに、エージェントが配備された箇所では不正経路広告を受信しないなどの不正経路広告元を切り離す技術について研究開発を実施する。

(到達目標)

経路ハイジャックを検知後、障害範囲の分析から回復及び不正経路広告元の切り離しまでを、数分以内に自律的に行う回復技術を確立する。

(ウ) 経路ハイジャックの予防技術

(技術課題)

経路ハイジャックは、日本においても過去大きな事例が数回発生しており、日常頻繁に発生している。AS 番号を取得する事業者等の増加に伴い、同様の事例が今後さらに増加する可能性があり、インターネット全体の経路の安定性の維持、制御を実現し、インターネットの安全性、信頼性を向上させるためには、経路ハイジャックを未然に防ぐ予防技術の確立が必要不可欠である。

しかし、現実的な予防技術は現在確立されておらず、経路情報の信憑性確認、検知、回復を含めた予防を可能とする IRR の基盤整備が必要不可欠である。

そのため、経路情報の信憑性を確認する IRR の安全性、信頼性を向上するために、IRR のリソースデータが正しくかつセキュアに登録、取得される認証システム、電子署名による信頼性向上技術の研究開発を実施する。また、関東近傍で発生した災害等により、一極集中で管理されている IRR の機能が失われないよう、IRR のスケーラビリティを確保するとともに、地理的に分散配備された IRR のセキュアなリソース伝播を可能とする技術の研究開発を実施する。さらに、各 AS におけるルータの経路情報を更新する際、IRR を参照し整合を確認した上で、適切に経路情報を更新する技術の研究開発を実施する。

(到達目標)

経路情報のマスターデータベースである IRR のリソースデータが 3 箇所以上の複数拠点に分散した環境において、不正な情報登録や誤った情報取得を防ぐ認証技術、及び高速かつセキュアなリソース伝播技術を確立する。また、IRR を参照してルータの経路情報を適時適

切に判断した上で自律的に更新する技術を確立する。

5. 実施期間

平成 18 年度から平成 21 年度までの 4 年間

6. その他

本研究開発の実施に当たっては次の点を考慮すること。

- ①経路ハイジャック対策技術として、国内外の ISP で広く実運用に供されることを視野に入れ、研究開発課題を選定し、研究計画を立てること。
- ②国内外の主要な IRR(レジストリが実施しているパブリックな IRR 等)との連携を効果的に実施して、研究開発を進めること。