経路ハイジャックの検知・回復・予防に関する研究開発

NTTコミュニケーションズ（株）NTT（株）、H18年度予算額1.7億円、H19年度予算額1.8億円、H20年度予算額1.8億円、H21年度予算額1.6億円

1. 研究開発概要

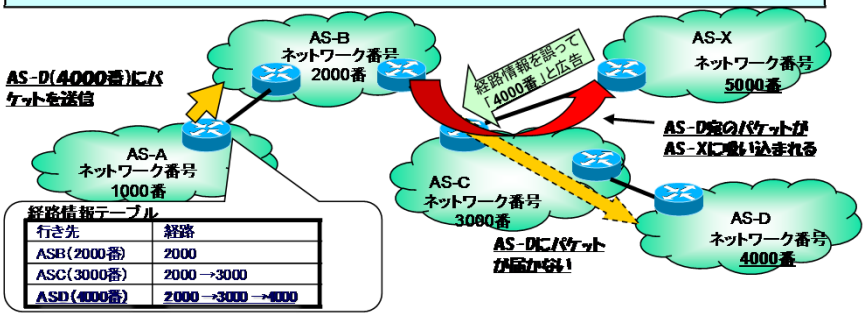
【目的】インターネットにおける経路情報の誤りによる通信障害（以下「経路ハイジャック」という。）を検知・回復・予防する技術を確立し、インターネットの安全性、信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境を実現する。

【政策的位置付け】「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。

【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、経路ハイジャックの迅速な検知、自律的な回復、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を実現する。

経路ハイジャックのメカニズム

AS-XがAS-Dのネットワーク番号（4000番）を誤ってAS-C等に広報することにより、AS-D宛のパケットがAS-Xに吸い込まれる。



2. 研究開発成果概要

(1)経路ハイジャックの検知技術

【目標】経路情報の確認を行うエージェントを各AS内に分散配置し、国内外で発生した経路ハイジャックを数分以内で検知できる経路監視技術を確立。

【成果】日本国内の全ISPとほぼ同数の600のASに分散配置したエージェントを連携させることにより、全エージェントからの経路ハイジャックの検知結果の通知が1分以内に完了することを確認。また、エージェント間流通情報の制限レベル（ASパスの公開・非公開）が異なるASの連携において、必要な機密性を確保した上でハイジャックの検知を可能とする方式について、複数の国内外のISPと協力して評価を実施し、実運用が可能であることを確認。

(2)経路ハイジャックの回復技術

【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報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。

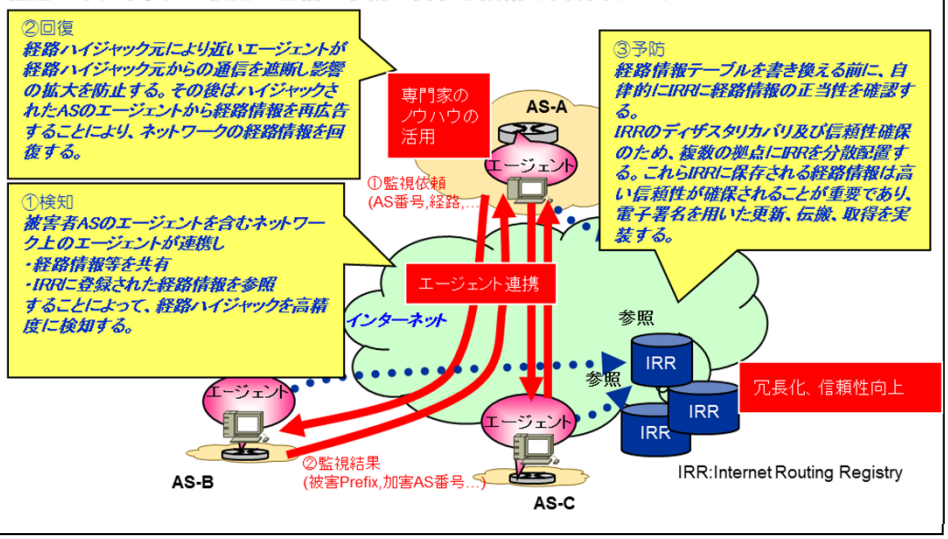
【成果】実際のインターネット環境において擬似的に経路ハイジャックを発生させた後、エージェントからの経路ハイジャックの検知情報をもとに、経路ハイジャック発生後の被害範囲や回復範囲を推定し、有効な回復措置（ハイジャックの経路切離し及び経路再広告）を自律的に、かつ、（アラート発生後）5分以内に選定・実行可能であることを確認。

(3)経路ハイジャックの予防技術

【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。

【成果】ディザスタリカバリを考慮し東京・大阪・福岡の3拠点に設置したIRRサーバ間におけるリソースデータの同期機能について、JPIRRを運用するJPNICの協力のもと、IRR運用上の観点から評価を行い、実運用性を確認した。また、電子署名等認証技術を用いたセキュアなIRRシステム及びクライアント環境を整備し、IRRシステムへの経路情報等インターネットリソースデータの登録、参照、他のIRRへのミラーリングの処理機能について、実用性を確認した。さらに、ルータが経路情報を受信した際に、自律的にIRRを参照し正常な経路を判別・制御し、ハイジャックを予防する技術を確立し、実証実験においてその有効性を確認した。

経路ハイジャックの検知・回復・予防に関する技術の実現イメージ



3. 研究開発成果の社会展開の状況

(1)経済的・社会的な効果

・本研究開発の成果である検知・回復技術については、Telecom-ISAC Japanや日本ネットワークインフォメーションセンター(JPNIC)といった通信業界団体と連携することにより、日本国内のISPへサービス展開を行うことが出来た。

・本研究開発で提起、実装された『高可用性』の考え方を利用して、新たな仕組みづくりへ寄与した。具体的にはRIPE NCC whoisサーバに反映・実装され、インターネットリソース管理DBの基盤を支えている。

(2)科学的・技術的な効果

・2012年にSnmp, Trapによる通知機能の追加、2013年にはIPv6にも対応するなど、技術力を向上させて汎用的なネットワーク管理システム(ネットワーク上に存在するネットワーク機器やサービスの監視および管理を行うシステム)との連携を柔軟に対応するなど、利用シーンの拡大を図ってきた。

・本研究開発成果である予防技術(IRR参照モデル)は、新しい要素であるRPKI(リソースPKI)技術を使った次のレベルの予防技術に進化した。RPKIは2013年に標準化(RFC 6811)されたが、本研究開発の研究メンバが標準化のドラフト作成に参加しており、新たな科学技術開発の誘因に寄与した。

(3)波及効果

・本研究開発での実証実験を契機に行われた企業間連携が現在も維持されており、そのため日本国内で発生する経路ハイジャックを広く検知する仕組みが確立されている。本研究開発の成果は、Telecom-ISAC Japanにて、経路情報共有WG(12ISP参加)において、2008年から実網検証が始まった「経路奉行」システムに活かされた。その後「経路奉行」はJPNICに2012年から移管され、現在も運営されている。

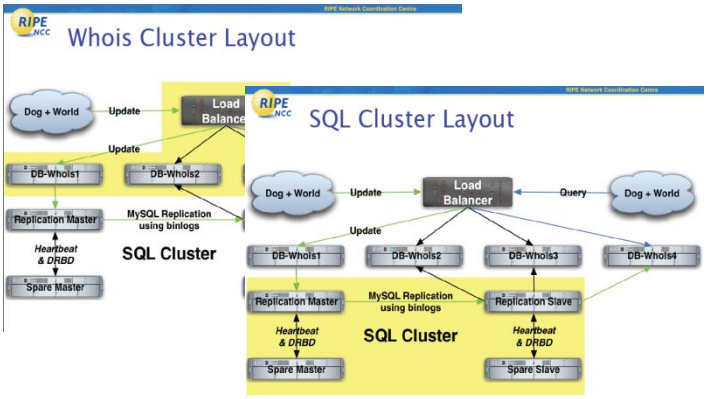
・本研究開発において企業間連携が確立したことにより、本研究開発の成果から誘引されたRPKI技術の重要性が共有され、企業間での技術の展開につながった。その結果、現在、RPKI技術は実用フェーズに至るまでとなった。

(4)その他

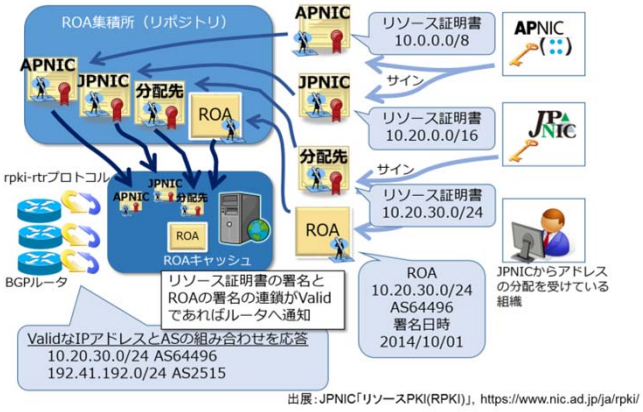
・5件の特許出願を実施、登録を受けた。(NTT)

・2010年2月Global IP Business Exchange 2010で「経路ハイジャックの検知・回復・予防に関する研究開発の取組と成果」を講演。(発表者:NTTコミュニケーションズ)

・2014年10月にヨーロッパ各国を中心とした主要IX及びIX関連団体が参加するイベントEuro-IX(第25回ルーマニア)において、IX事業者JPNAPで提供しているRPKIサービスや活動を紹介。



国際的な展開:RIPE NCC whoisサーバの取り組みに反映



RPKI(リソースPKI)を使用した予防技術に発展

4. 政策へのフィードバック

・本研究開発の成果により日本国内での経路ハイジャックに対するリスクは抑えられているものの、海外からのサイバー攻撃の脅威はいまだに存在する。
→今後は日本国外を含めた広範囲の対応が必要となる。海外を含めた多くのISPがエージェントを導入すれば、海外からのトラヒックも監視と対応が可能となり、結果として日本のインターネット環境が守られることとなる。そのためエージェントを広く海外展開することにより、日本国内のみならず日本国外を含めたインターネット環境の向上が期待できる。

・海外での展開については、各国のISPのみならず、ISPの先にいる顧客を巻き込むこととなるため、各国のISP間の連携が難しい状況となっている。また、各国ISPの技術レベルにもばらつきがあり、導入に困難が見られる可能性がある。
→海外への展開については、民間レベルのみでの対応が困難であるため、現在、欧米諸国はもちろんのこと、世界各国との連携体制の確立に向けた国レベルの働きかけを期待したい。また、広範な海外展開を実現するに当たっては、特にアジア諸国において、金銭面での負担が障壁となる可能性が高く、ODA等の積極的な経済支援政策が重要。加えて、技術者の育成やノウハウの移行等の支援が必要。