経路ハイジャックの検知・回復・予防に関する研究開発

R&D on Detection, recovery, and prevention technologies against the BGP Route Hijacking

研究代表者　南澤　正人　エヌ・ティ・ティ・コミュニケーションズ株式会社

研究期間　　平成 18 年度～平成 21 年度

This project titled “R&D on detection, recovery and prevention technologies against the BGP route hijacking” was aiming at wide deployment of its research results in not just only Japanese domestic but also international ISP (Internet Service Provider) s’ real operations. The first sub-project ″Detection technology against the route hijack″ enables operators to determine if the Internet route information carried by BGP protocol among ISPs is hijacked or not promptly. In the second sub-project ″Recovery technology against the route hijack″, an agent system which recovers the route automatically was planned to be implemented and evaluated in actual network settings.

In addition to these, the target of the third-part ″Preventive technology against the BGP route hijacking″ was the improvement of reliability of the route guidance information database with various techniques such as preventing the registration of illegal data to the database with cryptographic extension of the software and effective cooperation with IRR (Internet Routing Registry) worldwide.

The project has achieved successfully these goals - the fast reactive detection system of the route hijacking has been established, automatic recovery system has been verified, and illegal route guidance information registration could be prevented. The reliability and scalability of the route guidance information database has been improved. Autonomous validity securing of the route guidance information technology has been developed.

And, by installing these technologies into network nodes and network management system and evaluating in the real operation of the Internet, it is proved that results of this project have reached at practical level.

1　研究体制

○ **研究代表者**　　南澤　正人　（エヌ・ティ・ティ・コミュニケーションズ株式会社）

○ **研究分担者**　　瀬社家　光（日本電信電話株式会社　NTT ネットワークサービスシステム研究所）

○ **研究期間**　　平成 18 年度～平成 21 年度

○ **研究予算**　　総額　681 百万円

（内訳）

平成 18 年度	平成 19 年度	平成 20 年度	平成 21 年度
169.8	179.8	175.1	156.4

2　研究課題の目的および意義

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。

本研究開発では、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。

3　研究成果

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ため、経路ハイジャックの研究開発では、他のネットワークの保有している経路情報を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技術、検知の結果をもとに障害の要因と影響範囲の特定から、経路情報の誤りの回復に至るまでを自律的に行う技術、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に関する研究開発を実施し、迅速な検知、自律的な回復、不正な経路情報登録の防止等、経路情報データベースの信頼性向上等を実現した。

上記の技術確立に向けて、技術的な課題を抽出し、共同研究期間 2 社にて、下図に示す体制で研究開発を実施した。

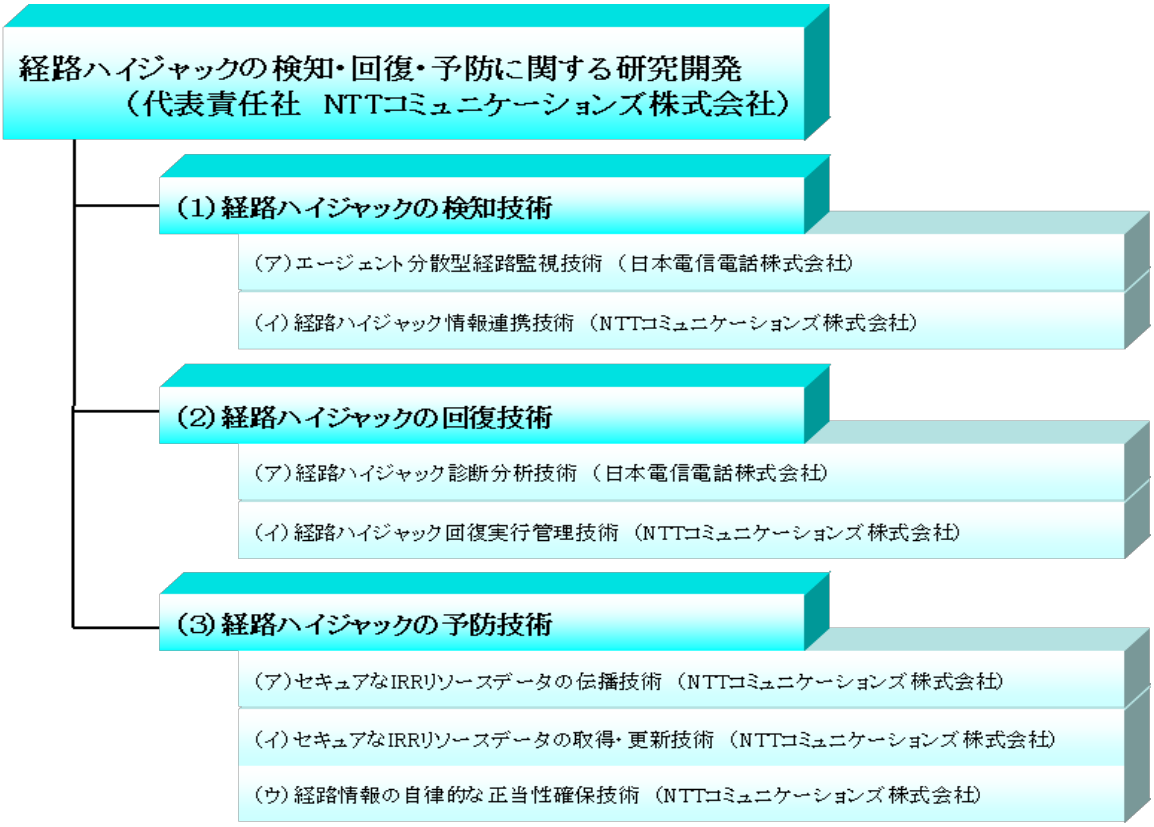


図 1　研究実施体制図

研究開発の成果については、図 2 に示すとおり、各年度毎にテーマを定め、各グループ毎に研究開発を実施した。

具体的には、検知技術では、インターネットで発生する経路ハイジャックを面的に監視するエージェント分散型経路監視技術を確立し、国内外 AS とインターネット上でその有効性を確認した。また、複数のエージェントで面的監視することで、経路ハイジャックの検知精度を向上させることが可能であることを確認した。回復技術では、経路ハイジャックを容易に回復させる手段として、分散型経路監視フレームワークを介して被害者 AS、中立 AS が協調して経路ハイジャックの回復処理を実施する「経路ハイジャック診断分析技術」の有効性を確認した。予防技術では、「セキュアな IRR リソースデータの取得・更新技術」の実装成果と、「セキュアな IRR リソースデータの伝搬技術」で確立された高可用機能の実装とを統合し、IRR システムをセキュア且つ高信頼なものにできることを確認した。また、「経路情報の自律的な正当性確保技術」では、ルータが経路情報を受信した際に、高信頼 IRR 基盤に登録されている IRR 情報を参照し、本来広告されてくる広告元からの正しい情報か否かを適切に判断した上で、ルータの経路情報を適切かつ自律的に更新を実施する仕組みを確立した。

さらに研究開発最終年度である平成 21 年度においては、Telecom－ISAC 等の協力のもと、フィールド評価として、経路ハイジャックの検知・回復技術のプロトタイプを複数 ISP、JPNIC 等と連携してインターネット環境に配置し、検知・回復技術のプロトタイプから予防技術のプロトタイプを参照させることで、検知・回復技術と予防技術の連携についての評価を実施し、有効に機能動作することを確認した。

上記以外にも「予防（ウ）：経路情報の自律的な正当性確保技術」では、Interop2009 の会場ネットワークにおいて、ルータより JPIRR データベースを参照し、ハイジャック被疑状態発生時の検出と制御が可能か評価を行った。また、インターネットの BGP 制御が行われている実環境において、東京、大阪拠

点をまたぐ広域な BGP 環境を構築し、経路ハイジャック予防機能の評価実験を行い、Interop と同様にハイジャック被疑状態発生時の検出と制御が可能であるという結果が得られた。

成果展開についても、研究進捗に合わせて適宜、国内外での外部発表（特許出願、論文/学会発表、報道発表、イベント出展等）を行った。

.

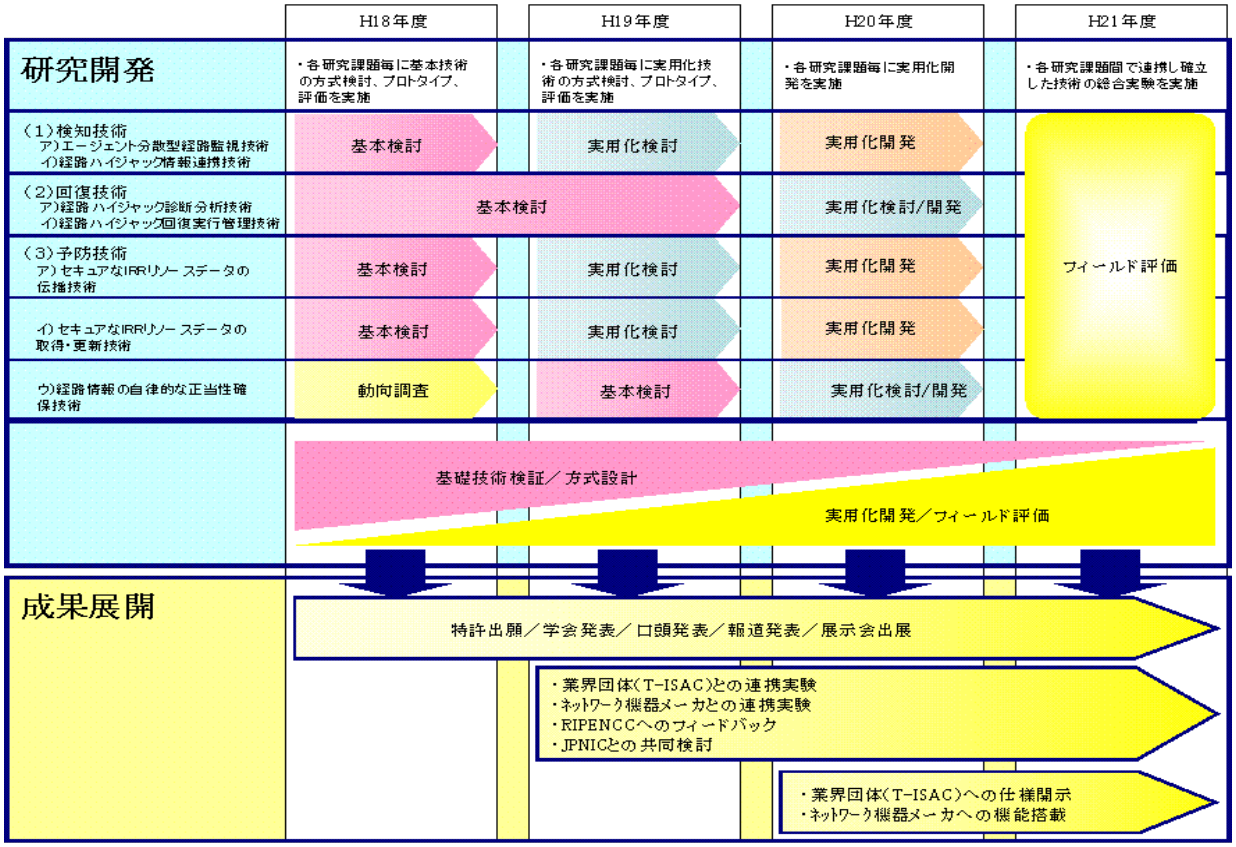


図２　研究開発計画と成果展開

３．１　経路ハイジャックの検知技術

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。

３．１．１　エージェント分散型経路監視技術

（目的）

国内外で発生する経路ハイジャックを迅速に検知し、その影響範囲を効率的に把握するために、インターネットで交換される経路情報を面的に監視し、それらの多くの観測ポイントから得られたデータを解析・分析し、経路ハイジャックを数分以内に自律的に検知するエージェント分散型経路監視技術を確立する。

（技術課題）

インターネットの経路情報を面的に監視するためにはエージェントを分散配置する必要があり、自律

分散したエージェントが協調して経路ハイジャックの検知を実現するには、以下のような技術課題がある。

分散配置したエージェントが協調して動作するために、エージェントがお互いに情報を流通させるための初期接続時の接続方式、エージェント間で監視の依頼、診断実施の依頼、監視状況の情報を交換するプロトコルが必要である。ここでは、多くのエージェントが連携することを想定し、そうしたときに連携先のエージェントが故障や障害でダウンした場合でも、全体には影響を及ぼさず動作可能で他エージェントへ擾乱を及ぼさない、といったことや、運用ポリシーの異なる多くの AS が参加可能であるような柔軟かつスケーラビリティのある連携技術である必要がある。

（提案手法）

エージェント分散型経路監視技術を確立するにあたっては、以下の点を考慮した技術の確立と、実際のインターネット環境あるいはインターネットを模擬したネットワーク環境でのシミュレーションによる本技術の評価が必要である。

1）連携先エージェントに提供する適切な監視対象経路情報の保障
2）分散配置された多数のエージェントの中から効果的な連携先エージェントの選択
3）連携エージェント数に対するスケーラビリティ

（実施内容・成果）

平成 18 年度は、経路ハイジャックの検知・回復を実現するプラットフォームとなるエージェント分散型経路監視技術の基本方式を確立した。多くの AS が参加容易であると同時に、耐障害性を兼ね備えた連携方式として、各 AS の観測ポイントであるエージェントが、経路監視サーバに接続することで、他の全ての経路監視エージェントとの協調連携監視が可能になるフレームワークを構築した。

平成 19 年度は、監視ポリシーが異なる AS 間で監視レベルを柔軟に設定可能とした連携モデルを採用し、多くの AS が参加しやすいフレームワークを構築した。同時に、参加 AS が増加した場合には経路監視サーバの負荷が増えるため、経路監視サーバの冗長化によるサーバの負荷分散を図り、数百のエージェントが協調動作可能なフレームワークを確立した。

平成 20 年度は、信憑性の高い高度な経路ハイジャック監視を行うために、署名技術を適用した IRR 予防技術との連携機能、分散したエージェントが協調してハイジャック真偽を判断するハイジャック診断機能、AS 詐称するような悪意ある経路ハイジャックを検出する AS パス妥当性診断機能を、協調連携監視フレームワーク上に実現した。また、平成 19 年から割り当てが開始された 4 バイト AS 番号に対応し利用シーンを拡大した。

平成 21 年度は、協調連携監視の公正な利用と検知情報の信頼性向上の観点から、経路情報の不十分な経路監視エージェントを協調連携監視から切り離し機能を実現し、IPv4 経路の枯渇問題により注目されてきた IPv6 経路に対しても、エージェント分散型経路監視技術が適用できることを確認した。平成 18 年度来確立してきた協調連携監視機能のフィールド検証を ISP10 社と連携して実施し、実際のインターネットで発生する経路ハイジャックを数分以内に検知可能であることを確認した。また、連携エージェントによる面的監視のスケーラビリティを確認するため、日本国内の全 ISP とほぼ同数の 600 エージェントによる協調監視の検証を実施し、全エージェントからのハイジャック検知通知が 1 分以内に完了することを確認し、本分散経路監視技術を用いた多地点からの経路ハイジャックの検知が可能であること

を確認した。

(まとめ)

4 年間の研究開発にて、インターネットで発生する経路ハイジャックを面的に監視するエージェント分散型経路監視技術を確立し、国内外 AS とインターネット上でその有効性を確認し、当初目標である「エージェント分散型経路監視技術」を確立した。

３．１．２　経路ハイジャック連携技術

(目的)

検知エージェントを複数拠点に配置し、経路ハイジャックの情報を速やかに該当 ISP へ通知する仕組みを確立するとともに、ISP 間でも共有可能な連携技術を確立する。

(技術課題)

インターネットを構成する各 AS 間での接続を行うルータの設定や運用ポリシーによる経路情報の追加・削除情報はリアルタイムに伝播しない場合がある。このような状況下では、経路情報の広告元 AS から遠いほど伝播遅延が発生することが予想され、広告元 AS から離れた AS における経路広告で経路ハイジャックされた場合には、途中での経路ハイジャック情報を検知することが必要である。

経路ハイジャックを検知するエージェントを複数箇所に配置した場合には、遠くに配置した検知エージェントが見つけた経路ハイジャックのアラート（警報）が遅延して到達したり、重複した経路ハイジャックのアラートが発生することで必要なメッセージが埋没してしまったりすることを考慮した通知技術が必要である。

また、面的に広がるインターネットでは、他 AS で発生した経路ハイジャックと無関係ではいられないため、ネットワーク全体における経路ハイジャックの発生状況・回復状況を知るために、各方面のエージェントから届いたデータを適切に処理し、経路ハイジャックの検知・回復状況を把握することが必要である。

(提案手法)

国内外を含めた経路ハイジャックの発生や回復の検知情報を集約する方式を確立する。これらの確立した技術をもとに、インターネットの実網において、経路ハイジャック情報連携技術の評価を行う。

(実施内容・成果)

平成 18 年度は、経路ハイジャックの検知技術における、(イ) 経路ハイジャック情報連携技術では、エージェントからの情報を集約（①アラート集約）し、ネットワーク上での経路ハイジャックの広がり状況を分析（②ハイジャック状態管理）し、オペレータが回復措置を実施する際の判断情報として提供する（③情報提供）までを、「アラート情報集約方式」として基本仕様を策定した。また、本集約方式をキーとした、「複数 ISP の連携による経路ハイジャック検知のフレームワーク」を提案した。

また、本研究での検知技術（ア）エージェント分散型経路監視技術に本検討を反映したプロトタイプシステムを用いて、ラボ環境でその有効性に関する基本的な評価を実施した。

平成 19 年度は、平成 18 年度に確立した「アラート情報集約方式」の実用性に関して、国内主要 ISP と連携してインターネット環境にプロトタイプシステムを適用し、本技術の展開に向けた課題(運用性、機密性など）についてヒアリング等による調査及び評価を実施した。

その結果、運用性については、各 ISP の運用体制の違いによる情報通知の種別選択及び通知タイミングの条件選択程度のカスタマイズ機能の具備で ISP 連携に向けた目処が立った。また、機密性については、不特定 AS（ISP）との連携を前提とするには、連携する ISP によってエージェント間で流通させる

経路情報に関して制御が必要であることから、情報流通制御による ISP 連携スキームに関する要件を整理し、ISP 連携スキームの方式提案を行い、ISP 連携監視の普及に向け ISP が参加しやすい連携形態及びその対応方式についての見通しを得た。

平成 20 年度は、平成 19 年度に引き続き、経路ハイジャックを監視する基盤技術の実用性に関して、国内主要 ISP と連携してインターネット環境に本方式のプロトタイプを適用し、本技術の展開に向けた課題（運用性、機密性など）についてヒアリング等による調査及び評価を実施した。

その結果、複数の国内外 ISP が経路ハイジャック監視において連携する際の各 ISP エージェントの連携レベルを、AS パス変化情報まで流通する・AS パス変化情報は隠蔽する・情報流通を行わない、の 3 つの連携レベルで評価を行い、本方式による運用が可能であることを確認した。また、連携 AS を Tier1 AS に拡大することにより、国内のみにエージェントを設置した場合に比べ、BGP ルータが受信する経路情報が増加し、受信経路情報の拡大が検知精度の向上に繋がるという見知を得た。

一方、今後発生しうる悪意ある経路ハイジャックとして考えられる“オリジン AS 詐称による経路ハイジャック”の検知技術を検討し、方式評価を実施した。

平成 21 年度は、平成 20 年度に達成した実用化研究開発成果について、国内外 ISP と協力して評価を実施し、面的監視技術の評価や普及を進めるために必要な課題の抽出を実施した。また、平成 20 年度までの研究成果、並びに検知技術と回復技術、予防技術との技術間連携評価や本技術の普及を円滑に行うための評価を国内外 ISP を交えて実施した。

その結果、複数のエージェントで面的監視することで、経路ハイジャックの検知精度を向上させることが可能であることが確認できた。また、検知、回復、予防技術を組み合わせた評価を行い、予防技術(ア)（イ）の研究成果である高信頼 SecureIRR システムとの接続機能を確認し、経路ハイジャックの発生や回復の検知情報を集約する方式を確立することができた。

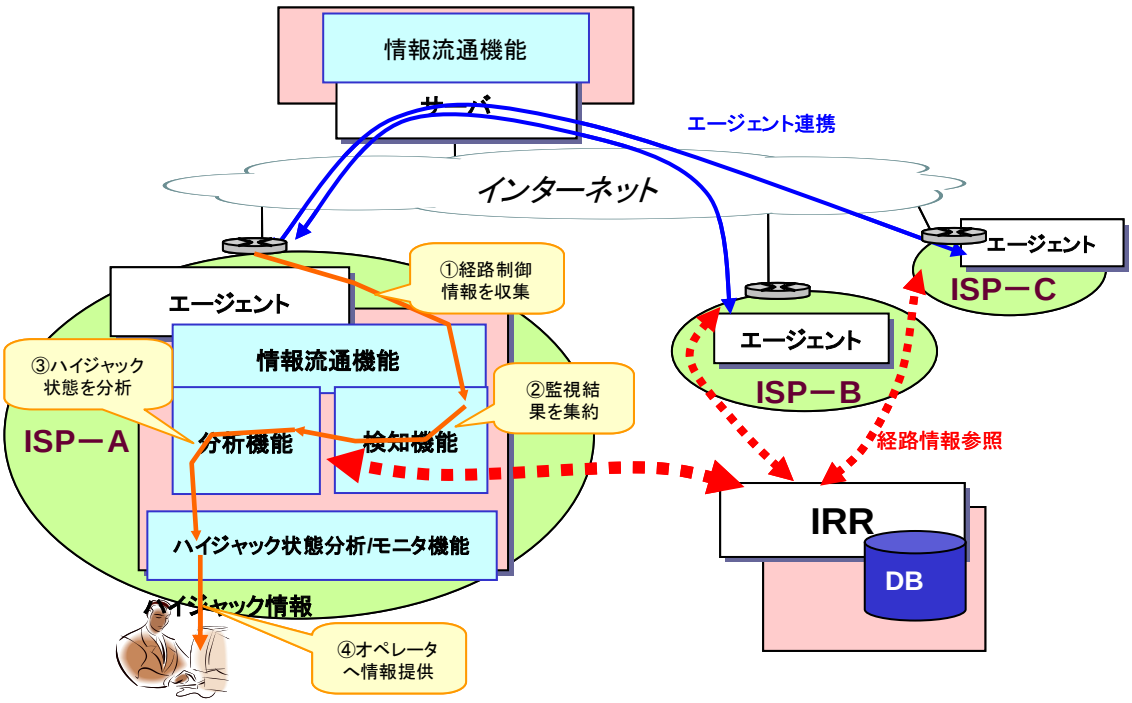


図３　エージェント分散型経路監視技術の概要図

３．２　　経路ハイジャックの回復技術

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。

３．２．１　経路ハイジャック診断分析技術

（目的）

スキルが高くないオペレータでも経路ハイジャックが発生した場合に容易に対処できることを目的として、経路ハイジャックの影響状況についての情報を提供するとともに、自律的な通信障害の回復を実現する経路ハイジャック診断分析技術を確立する。

（技術課題）

経路ハイジャックが発生した場合、現状では、不正な経路広告元の特定や誤った経路広告の停止等の回復作業は人手を介して行っているため、多大な時間を要している。このため、エージェントには、自律的に経路ハイジャックの状況を診断し、通信障害を回復させる技術が必要である。また、エージェントが回復プロセスを自律的に行うためには、どの経路に対してどのような経路制御を行うかを分析・決定する必要がある。その際には、経路ハイジャックにおける加害者 AS・被害者 AS・中立的 AS によって回復手順が異なることなどを考慮する必要がある。経路ハイジャック診断分析技術を確立するにあたっては、複数のエージェントから得た情報をもとに経路障害の範囲などを分析し、不正経路の切り離しや正しい経路の再広告を自律的に実施する技術の確立が必要である。

（提案手法）

複数エージェントから得られる情報をもとに障害範囲などを分析し、エージェントが配備された AS では不正経路を切り離すことや正しい経路の再広告を自律的に実施することで経路ハイジャックを回復する技術の確立を目指す。具体的には、下記のようなエージェントからルータに対して回復手順を指示する技術方式設計を行い、評価を行う。

1）　加害者 AS では、正しい経路の再広告や誤った経路の広告停止等
2）　被害者 AS では、正しい経路の再広告や最長一致法を利用した広告等
3）　中立的 AS では、誤った経路を受信しないなどの経路フィルタ等

（実施内容・成果）

平成 18 年度は、エージェント分散型経路監視技術の同プラットフォームを用いて、経路ハイジャックを自律的に回復するための基本方式を検討した。被害者 AS にて行う「ハイジャック経路の再広告」と、ハイジャックを検知した中立的 AS で行う「ハイジャック経路の切り離し」が、ハイジャック発生後緊急で実施する暫定対処方法として有効であると方向付けた。

平成 19 年度は、「ハイジャック経路の再広告」を行うための機能をエージェント分散型経路監視フレームワーク上に実現した。回復有効範囲の最大化と同時に、AS のフィルターポリシーやインターネットに及ぼす副作用を最小化する方式として、Exact 経路広告、Longer 経路広告の 2 段階の再広告法を実現し、た。また、検知技術による経路ハイジャックの検出後、自律的に回復技術と連携し、回復措置実行やその実行結果を検出する検知技術と技術連携しハイジャック経路を再広告する技術を確立、有効性を

確認した。

平成 20 年度は、「ハイジャック経路の切り離し」を行うための機能を平成 19 年度版エージェント分散型経路監視フレームワーク上に実現した。被害者 AS と中立的 AS が協調することでハイジャック経路の広告範囲を限定し、ハイジャック汚染範囲を切り離す技術を確立し、その有効性を確認した。

平成 21 年度は、「ハイジャック経路の再広告」時の AS フィルターポリシーによりフィルタされる影響を軽減させるため、回復処置を支援する仕組みとして再広告経路を IRR へ登録する機能を実現した。平成 18 年度来確立してきたエージェント分散型経路監視フレームワーク上の回復技術について ISP10 社と協力してフィールド検証を実施、インターネット上で発生する経路ハイジャックに対して回復機能が有効に機能すること、回復段階における各連携エージェントからの回復通知によりハイジャックの影響範囲が把握可能であることを確認した。

以上より、経路ハイジャックを容易に回復させる手段として、分散型経路監視フレームワークを介して被害者 AS、中立 AS が協調して経路ハイジャックの回復処理を実施する「経路ハイジャック診断分析技術」の有効性を確認した。

３．２．２　経路ハイジャック回復実行管理技術

（目的）

経路ハイジャック状態を検知した場合、エージェント経由の対話形式で様々な情報を確認しながら、ルータへの経路制御支援を行う回復手順の実行管理技術を確立する。

障害要因と影響範囲の特定データをもとに、経路情報の広告誤りに対する回復手法を自律的に実施する技術を確立する。

（技術課題）

経路ハイジャックの回復措置はネットワーク管理者の BGP オペレーション技術に依存しており、現状では国内でも技術者が多くない。従って、専門家のノウハウを活用できるスキーム、及び、簡易なケースやパターン化されたケースにおける短時間での回復技術が必要である。そのためには、(ア) 経路ハイジャック診断分析技術で分析された診断結果をもとに、各 AS の運用ポリシーに応じた、経路制御を行う回復手順の実行管理を確立しなければならない。

（提案手法）

回復手法の調査を行い、回復対処可能な設定手順やルータコマンドを実行する仕組みを実装し、各 AS での運用ポリシーに沿ったカスタマイズが可能な自律的な回復技術を確立する。

（実施内容・成果）

平成 18 年度は、経路ハイジャックの被害者 AS のオペレータが回復措置を実施する際の実行管理環境及びその効果の評価環境構築に向け、経路ハイジャックの被害範囲（感染範囲）を複数の観測ポイントに配置された検知エージェントからのアラート情報をもとに推定し、その情報をオペレータに提供する（①経路ハイジャックの回復状態管理）こと、回復措置の実行状況とその回復状況を管理する（②回復手順シナリオ選定と実行管理）ことをベースにした回復手順シナリオの方式の検討を行い、基本方式設計書としてまとめた。

平成 19 年度は、平成 18 年度の研究成果技術（回復技術（ア）及び（イ）における 2 段階方式の経路再広告、回復状態管理などの要素技術）を組み合わせた自律的回復技術の有効性をプロトタイプ版で検証した。また、一般に経路のインターネット上での伝播の仕方は、取り巻く AS の経路広告ポリシーによ

って異なることから、“2 段階方式の経路再広告による経路ハイジャックの部分的回復手段”の実施に際しては、AS 毎の事情に応じた回復マネジメントが必要であり、被害者 AS を取り巻く事情（AS の経路広告ポリシー、接続関係、など）による回復措置アクションの利き方を視覚化し、アクションによる回復状況（有効性）やその限界（アクションが利かない範囲）に関する結果の分析技術を提案することで、自律的回復技術の高度化を具現化した。

平成 20 年度は、平成 19 年度までに検討した自律的回復技術の研究成果を評価するため、平成 20 年度に回復技術（ア）の成果「ハイジャック経路の切り離し」を組み合わせた自律的回復技術の有効性をプロトタイプ版で検証した。また、ハイジャック被害状況の分析及び適切な回復措置を誘導・支援する統合管理方式の検討を行い、ハイジャック発生から解消までの一連のイベントや作業に関する分析技術を提案することで、回復マネジメント技術の高度化を具現化した。

平成 21 年度は、平成 20 年度までに開発したプロトタイプを用いて、回復技術の有効性を、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ることにより評価した。具体的には、検知エージェントのアラート情報をもとにした経路ハイジャック発生後の“被害範囲/回復範囲推定”や、被害状況に応じて有効な回復措置を自律的に選定・実行する“回復手順シナリオ選定と実行管理”が有効に機能することを確認した。ハイジャック発生検知後から 5 分以内に回復措置を実行し、その回復措置の結果が把握できること、及び経路ハイジャック回復オペレーションについての有効性の評価を国内外 AS を交えて実施し、当初目標の「経路ハイジャック回復実行管理技術」を確立した。

３．３　　経路ハイジャックの予防技術

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。

３．３．１　IRR リソースデータデータ伝播技術

（目的）

日本のパブリックな IRR である JPIRR を含め、現在の IRR の多くは 1 箇所で集中管理されており、災害対策などを考えると本格的に IRR を利用していくには、分散環境を整備する必要がある。

その際、現在の IRR は、そのリソースデータの伝播方式において脆弱であるため、高速かつセキュアにリソースデータを伝播できる技術を確立する。

（技術課題）

現在の IRR 同士のリソースデータの交換は、ミラーリングと呼ばれ、単にデータを丸ごと交換しているような状態であり、これを改善する必要がある。また、IRR の情報をもとにルータの経路情報の更新に適切に反映することを踏まえると、その元情報、つまり経路情報の台帳を担う IRR の情報伝播はスケーラブルに行われる必要がある。

（提案手法）

高速かつセキュアなリソースデータの伝播技術を確立するためには、伝播する技術を２つに分類する必要がある。

１）同一 IRR 管理組織内での IRR リソースデータの同期技術

２）異なる IRR 管理組織間での IRR リソースデータの同期技術

１）については、データベースクラスタリング技術を IRR システムへ応用することにより、現在のミラーリング技術を高速かつスケーラブルなものにする。またリソースデータの伝播の際に、暗号化技術を適応することにより、セキュアなリソースデータの伝播技術を確立する。

２）については、既存のミラーリングシステムに影響を与えることなくスムーズなマイグレーションを実現する技術を確立する。

（実施内容・成果）

平成 18 年度は、IRR リソースデータの伝播を可能とするセキュアな IRR リソースデータの伝播技術を研究し、新しい IRR の基本設計・詳細設計を行い、プロトタイプ版の IRR を開発し、評価を行った。

平成 19 年度は、平成 18 年度に開発したプロトタイプ版の IRR を発展させた本格版を開発し、機能・性能評価を実施した。実際にディザスタリカバリを考慮した東京・大阪拠点を構築し、分散した環境下においても IRR サーバ間のデータ同期や冗長性を担保したシステムを開発し、一定の成果を得た。

平成 20 年度は、平成 19 年度に開発した高可用 IRR システムについて、IRR システムの配置方法（拠点内、拠点間同期）に関する検討を行い、性能向上を目的とする改造を実施した。また、IRR システムを 3 拠点（東京、大阪、福岡）に設置し、性能への影響等の評価を実施した。また、併せて、JPIRR を運用している JPNIC の協力のもと、IRR 運用上の観点からの評価を実施した。

平成 21 年度は、高可用 IRR システムに性能向上を目的とする改造を実施した平成 20 年度版 IRR システムに「(イ)セキュアな IRR リソースデータの取得更新技術」との結合を行い、高信頼 SecureIRR システムを実装した。

また、最適拠点選択機構として、RTT の短い最適な拠点を選択する機能を実装した。

さらに、フィールドトライアルを行い、トライアルユーザからの参照・登録更新の確認については、問題なくアクセスが可能であることを確認し、擬似故障トライアルについては、運用担当者として想定した JPNIC により故障対応が行われ、スムーズな対応により、故障を回復できることを確認し、当初目標であった「セキュアな IRR リソースデータの伝播技術」を確立した。

３．３．２　セキュアな IRR リソースデータ取得・更新技術

（目的）

現状の IRR はインターネットリソースデータ（以下、リソースデータ）の登録において、メンテナーとして登録権限を有していれば、インターネットレジストリなどから正規に割り当てられたリソースデータ（例えば、経路情報など）以外でも登録・更新することができてしまう。このため、本来のリソースの保有者以外が情報を不正に登録・更新することが可能な脆弱性があるといえる。IRR に蓄えられる情報の信頼性を高めるために、これらの状態を改善する技術を確立する。

また、IRR に登録されたリソースデータは、他の IRR に情報がコピー（ミラーリング）され分散管理される。ミラーリング先においても、オリジナルなデータと同等の情報であることを担保する技術を確立する。

（技術課題）

IRR の情報が安全にかつ正確に登録されたとしても、オペレータに代表される第三者が参照した場合に、IRR に登録されている情報が本当に正しい情報か否かを確認する手段がない。

（提案手法）

IRR に登録する情報（オブジェクト）の正しさを担保すること、また、オブジェクトに対し電子証明技術を適用し、他人が参照した際や登録の際に、正しさが確認できる認証システムを確立する。

（実施内容・成果）

平成 18 年度は、登録する IRR リソースデータが正しい登録者による登録かどうかを判別可能とするため、セキュアな IRR リソースデータの取得・更新技術の基本設計を行った。

平成 19 年度は、登録、ミラーリング、そして参照の各フェーズでのセキュア化の検討、詳細設計を実施した。登録においては、S/MIME によって信頼性の高い認証と登録内容の改竄防止を図ると同時に、インターネットレジストリによって割り振られた IP アドレス範囲でルートオブジェクトが登録されることを担保した登録方式（「セキュア登録」）、ミラーリングにおいては、TLS（相互認証）を利用したミラーリング方式（「セキュアミラー」）、そして参照においては、電子署名を利用し、参照者が電子署名を検証することによってミラーリングにより複製されたオブジェクトであっても改竄を検知できる参照方式（「セキュア参照」）の詳細設計を実施した。また、電子署名モジュールのプロトタイプ開発を実施し、電子署名技術の IRR システムへの影響、ならびに参照者側における影響を定量的に評価した。

平成 20 年度は、既存の IRR システム（RIPE Whoisd）に対し、平成 19 年度の検討をもとに、IRR システムへの登録、参照、及びミラーの、それぞれの項目に対してセキュア化の処理を施すシステム開発を行い、性能測定を実施した。また、IRR システムに蓄積される経路情報を清浄にするには、インターネットレジストリが保有する IP アドレスの割振り、割当て情報と整合が取れている事が重要と捉え、日本におけるインターネットレジストリである JPNIC とシステム連携について検討し、システム（Secure IRR システム）の実装に反映した。（図４）

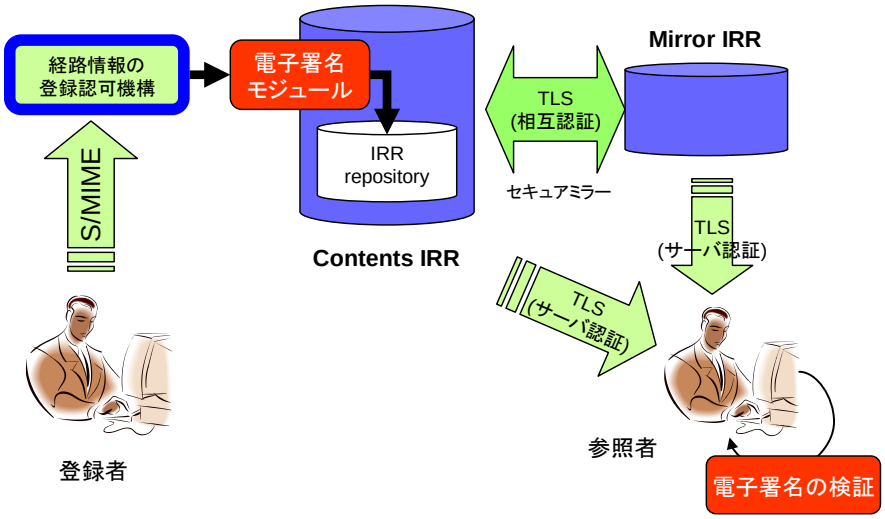


図４　Secure IRR システム概要図

平成 21 年度は、平成 20 年度までの「(イ) セキュアな IRR リソースデータの取得・更新技術」の実装成果と、「(ア) セキュアな IRR リソースデータの伝搬技術」で確立された高可用機能の実装とを統合した、高信頼 SecureIRR システムを実装した。また、実証実験や実用化を考慮し、高信頼かつセキュアな IRR システムを利用するためのクライアント環境を整備した。加えて、JPNIC が開発、運用している「経路情報の登録認可機構」との接続性を確認する事と、インターネットオペレータからの定性的な評価を得る事を目的とし実証実験を実施し、当初目標であった「セキュアな IRR リソースデータの取得・更新技術」を確立した。

３．３．３　経路情報の自律的な正当性確保

（目的）

インターネット上で交換される BGP の経路情報は、ある一定の経路フィルタに基づき交換され、ルータは自律的に経路情報の更新を行っている。その際、誤った経路広告が発生した場合、現状では他のルータから受信した BGP の経路情報の正当性をきちんと評価せずに受信してしまい、一定の経路フィルタを通過してしまった場合、誤った経路情報に基づいて情報更新を行ってしまうという問題がある。

本技術研究開発では、(ア) セキュアな IRR リソースデータの伝播技術と（イ）セキュアな IRR リソースデータの取得・更新技術によって確立された IRR 基盤技術に基づき、経路ハイジャックの発生を未然に防ぐ、自律的な経路ハイジャック予防を実現する経路情報の正当性確保技術方式を確立する。

（技術課題）

ルータの経路情報と IRR のリソースデータとが連携し、ルータが正当な経路情報のみを更新する仕組みは確立されていない。また、その他検討されている方式も幾つか存在するが、まだ確立された技術は存在しない。

（提案手法）

ルータが経路情報を受信した際に、高信頼 IRR 基盤に登録されている IRR 情報を参照し、本来広告されてくる広告元からの正しい情報か否かを適切に判断した上で、ルータの経路情報を適切かつ自律的に更新を実施する仕組みを確立する。

（実施内容・成果）

平成 18 年度は、「セキュアな IRR リソースデータの伝播技術」と「セキュアな IRR リソースデータの取得・更新技術」の２つの技術を組み合わせて管理される IRR リソースデータを用い、経路情報を受信した際に、ネットワーク機器が自律的に正常な経路を判別・制御する経路情報の自律的な正当性確保技術の確立に向けた関連技術調査研究として、セキュア BGP 関連プロトコルの最新技術動向調査、証明書技術の標準化最新技術動向調査、経路ハイジャックの実情及び BGP 全般のセキュリティ脅威と対応策に関する調査研究を実施し、次年度以降の基礎検討を行った。

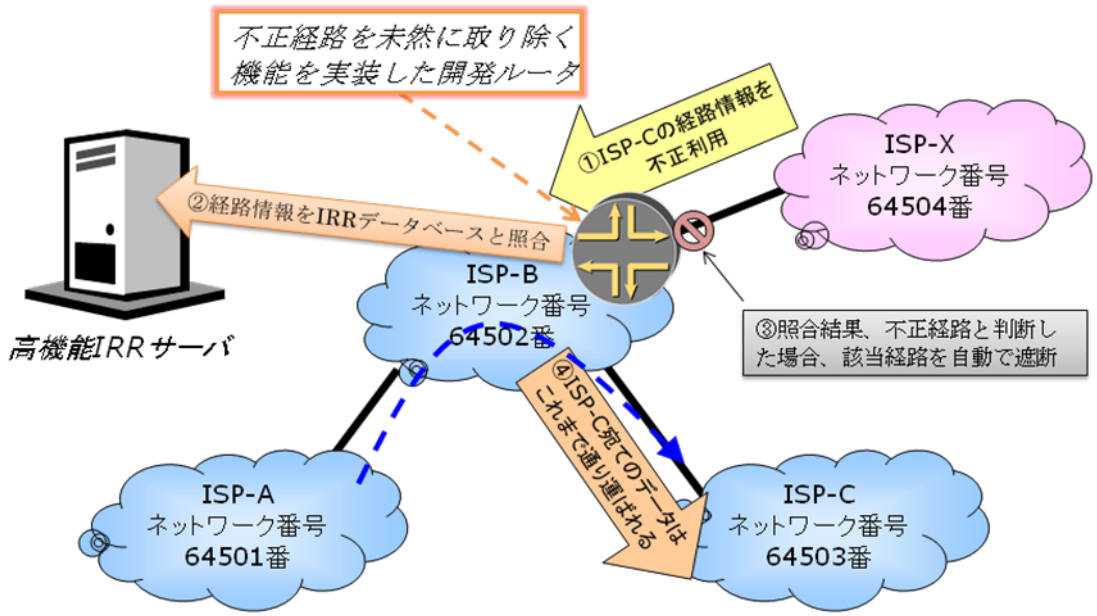
平成 19 年度は、実際にルータに予防機能を搭載する際の設計を Juniper 社及び Cisco 社の主要な２大ルータメーカの BGP アーキテクトと意見交換を行いながら実施し、ルータが IRR システム参照時にハイジャック経路と判定し予防すべき「ハイジャック経路」の整理、ネットワークの自律的な正当性検証方式の全体像の整理、IRR システムとルータ機器の処理の流れの解析、及び各フェーズに分類して経路情報の正当性確保を実現するための要件整理を実施し、予防アーキテクチャの基本設計を行った。

平成 20 年度は、平成 19 年度の基本設計をもとにネットワーク経路制御を行う BGP ルータが、経路情報の受信時に IRR システムに登録された経路情報を参照し、その情報をもとに経路情報の正当性の確認を行い不正な経路情報の混入を防ぐ方式の詳細な検討の実施、プロトタイプ実装・評価を行った。改善すべき課題はあるものの、ネットワーク上での予防機能の動作を確認することができ、IRR データベースとルータが連携した予防機能を実現した。

平成 21 年度は、昨年度の課題と知見をベースに詳細設計、実装の改善を行い、経路ハイジャック予防モジュールの本格開発を行った。結果、当初目標であった自律的な経路ハイジャック予防を実現する正当性確保技術を確立した。また実証実験を行い、本技術の有効性を確認した。

標準化については、SIDR (Secure Inter-Domain Routing) WG にて標準化を推進し、経路情報の正当性検証方式を規定したインターネットドラフト「draft-pmohapat-sidr-pfx-validate-07」へ反映を行い、

本技術開発メンバが Contirbutor として連盟し、標準化への取り組みが前進した。また、株式会社 ACCESS の米国子会社である IP Infusion の BGP ルータ「ZebOSR Internet RouteServer」へ本研究開発にて確立された正当性確保技術が実際に組み込まれるに至り、製品ルータへ導入された。



①ISP-XがISP-Cの経路情報を不正に利用

②本開発ルータが自動的に該当経路情報に基づき、IRRデータベースに照合を実施

③照合結果、不正経路と判断された場合には、本開発ルータが自動で不正経路を遮断

④ISP-C宛てのデータはこれまで通り問題なく運ばれる

図５　経路情報の自律的な正当性確保技術概要図

３．４　　その他研究実績

３．４．１　検知・回復・予防技術フィールド実験

１．フィールド実験（検知・回復＋予防（ア）、（イ））

平成 21 年度においては、平成 20 年度までに開発した経路ハイジャックの検知・回復技術のプロトタイプを用い、「経路再広告」と「ハイジャク経路の切り離し」による回復技術の有効性を、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ることにより評価を実施した。

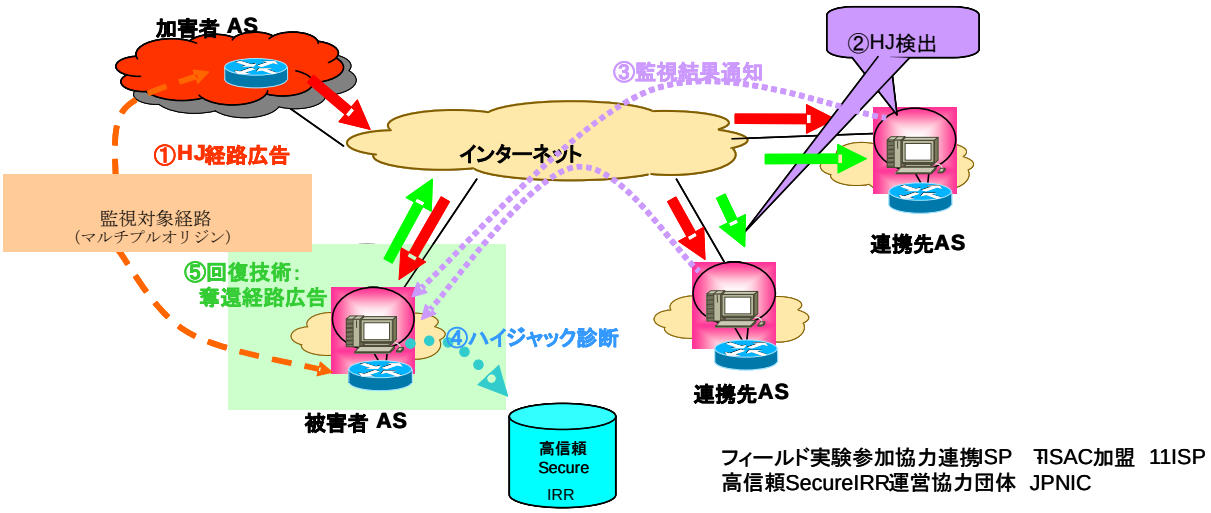


図 6　検知回復予防フィールド実験

また、経路ハイジャックの予防技術の研究の成果である、セキュアな IRR リソースデータの伝播を可能とする「(ア) セキュアな IRR リソースデータの伝播技術」と、登録する IRR リソースデータが正しい登録者による登録かどうかを判別可能とするための「(イ) セキュアな IRR リソースデータの取得・更新技術」を結合したトライアル版を作成した。これを実際のインターネット環境に設置し、経路ハイジャックの検知・回復技術のプロトタイプを複数 ISP、JPNIC 等と連携して、検知・回復技術のプロトタイプから予防技術のプロトタイプを参照させることで、検知・回復技術と予防技術の連携についての評価を実施し、有効に機能動作することを確認した。

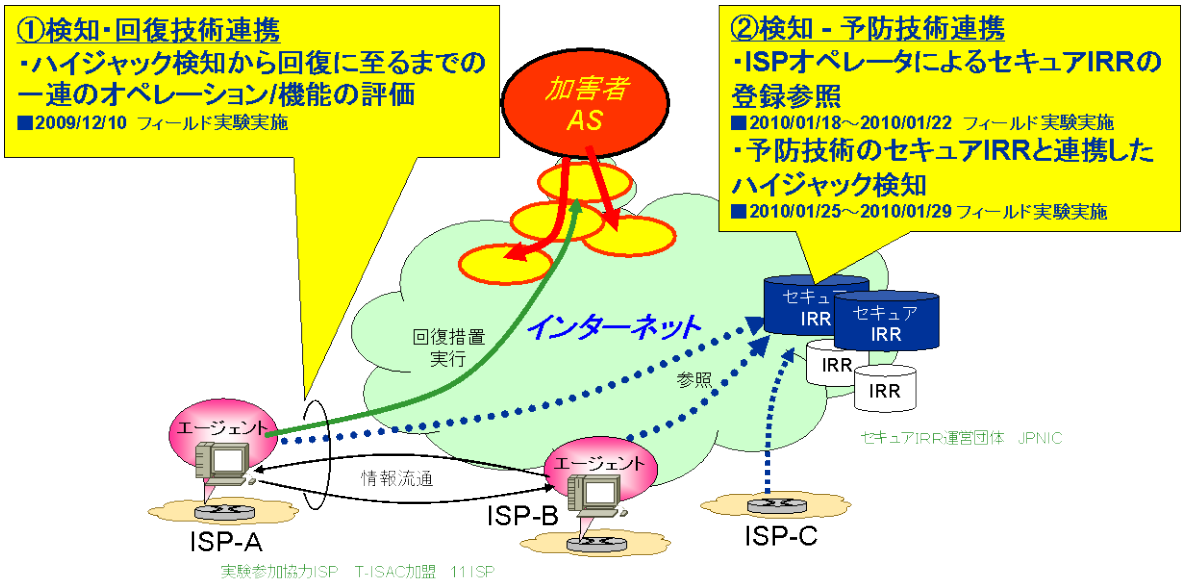


図 7　フィールド実験

さらに、予防技術の個々の技術要素及び検知・回復と予防の連携した上での展開に向けた課題につい

て、フィールド実験参加者へのヒアリング等による調査及び評価を実施した。

２．フィールド実験　（予防（ウ））

予防フィールド実験（1）

Interop2009 の会場ネットワークにおいて、会期中（5 日間）に本機能の評価を実施した。Internet フルルートを予防ルータ（図中枠で囲った hijack ルータ）へ伝搬し、ルータより JPIRR データベースを参照し、ハイジャック被疑状態発生時の検出と制御が可能かを評価した。会期中に合計 3 件のハイジャック被疑状態を検出し、ハイジャックの実質的被害は観測されなかったものの、予防ルータの動作としては何れも良好な結果が得られた。

表１　Interop2009 ShowNet での検出結果

BGP 観測 prefix	BGP 観測 origin AS	IRR 登録 prefix	IRR 登録 origin AS
133.170.0.0/16	AS4732	133.170.0.0/16	AS4713
113.213.242.0/23	AS9371	113.213.240.0/22	AS9370
210.171.224.0/24	AS7473	210.171.224.0/20	AS7527

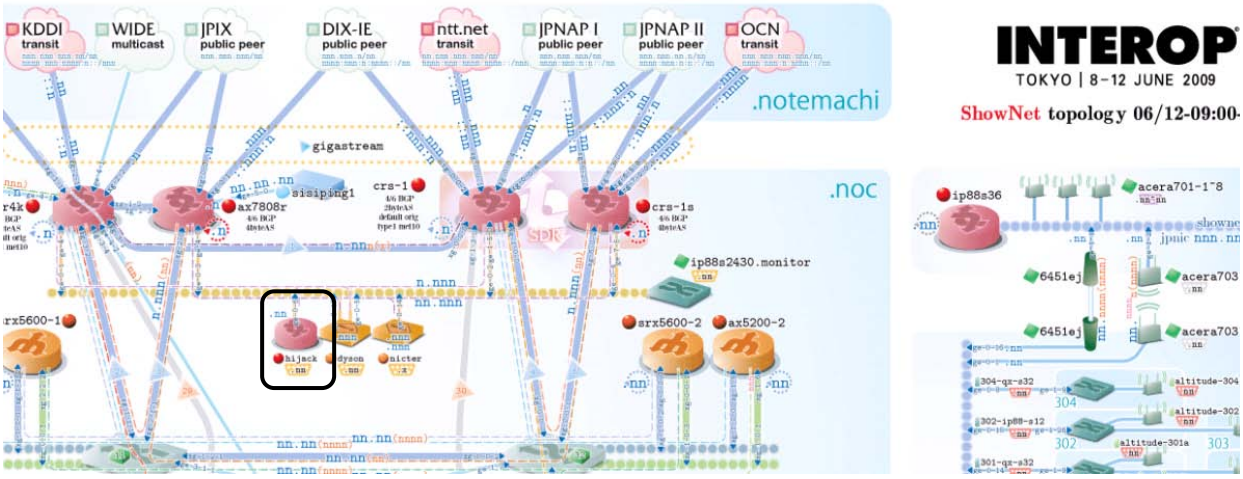


図８　Interop2009 ShowNet トポロジー構成

予防フィールド実験（2）

インターネットの BGP 制御が行われている実環境において、東京・大阪拠点をまたいだ広域な BGP 環境を構築し、経路ハイジャック予防機能の評価実験を行った。IPv4 に関しては大阪の AS37923 よりハイジャック状態を発生させ、東京の AS18131 にて意図した形で予防が可能であることを確認した。また IPv6 予防機能に関しても正常に動作することを確認した。

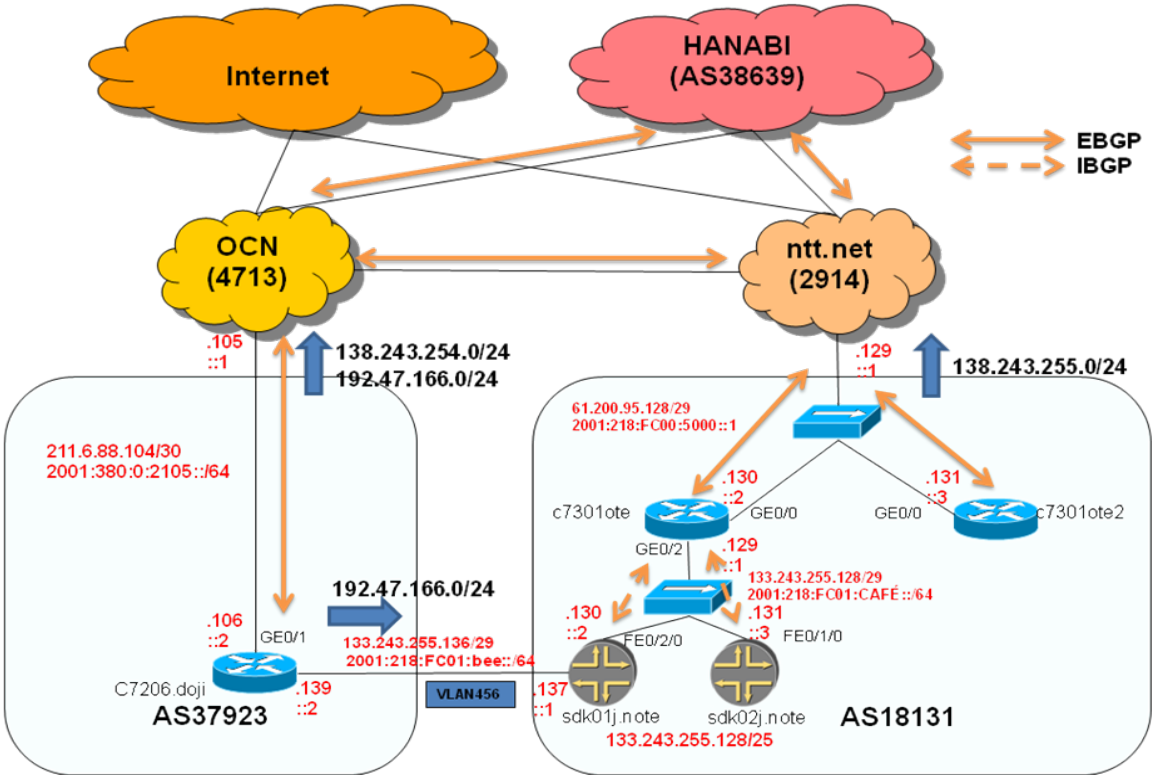


図９　実験構成図

実際に予防を実施した際の課題としては、今回のケースも含め、観測される事象の多くの場合は、データベースへの登録漏れなどによる誤検出、誤制御となる場合も少なくないため、例えばすぐに予防制御できる状態の手前の設定状態に自動的に制御し、その後ケース毎に運用でカバーする、あるいは経路ハイジャック被疑状態と検出された経路については、ルータ内の priority を落とした形で経路制御を実施するなどの対策を実施するなどが望ましい。また、データベースへの登録に関しても、様々なデータベースが運用されている状況での制御が必要となってくるため、最終的には参照データベースの統一化が課題である。日本の場合、JPIRR データベースが現状マスターデータベースとして機能しつつある状況にある。

３．４．２　研究成果の普及・促進活動

本研究開発において、業界団体 Telecom-ISAC と共同実験を実施し、得られた検知・回復技術に関するノウハウ・知見を Telecom-ISAC に展開した。

また、今回開発した予防技術（高信頼 IRR 技術）をヨーロッパ、中近東、アジアの一部を受け持つ地域インターネットレジストリであり、その地域の IRR システムである RIPE Whois サーバを開発・運営する RIPE NCC へ技術提供した。

さらに、予防技術（IRR 自律参照機能）が ACCESS 米子会社 IP Infusion のルータ OS(zebOS®)に搭載され、本研究開発で得られた知見や成果が実製品へと反映された。

なお、本研究開発の進捗に応じ、特許申請を５件実施し、これまでに「経路情報生成広告方法、経路情報生成広告装置及び経路情報生成広告プログラム（特許 04365868)」、「経路情報変更方法、経路情報変更装置及び経路情報変更プログラム（特許 04365869)」の２件について特許を取得した。

また、本研究開発の成果については、年度毎の研究進捗に合わせて APRICOT 、RIPE Meeting、電子情報通信学会等での講演などの対外的な外部発表を実施した。

4　研究成果の更なる展開に向けて

本研究開発で得られた技術及びノウハウを広く業界に向けて普及を進める。

本研究開発において、業界団体 Telecom-ISAC と共同実験を実施し、得られた検知・回復技術に関する技術仕様の開示を実施する。

エヌ・ティ・ティ･コミュニケーションズ株式会社のインターネットサービス（OCN）,海外向け IP ネットワーク（GIN）への実装を進める。

今回開発した予防技術（高信頼 IRR 技術）をヨーロッパ、中近東、アジアの一部を受け持つ地域インターネットレジストリであり、その地域の IRR システムである RIPE Whois サーバを開発・運営する RIPE NCC へ技術提供を実施していく。

また、予防技術（IRR 自律参照機能）が ACCESS 米子会社 IPInfusion のルータ OS(zebOS®)に搭載され、本研究開発で得られた知見や成果が実製品へと反映された。さらに、Juniper 社のルータ OS(JUNOS®)を利用したルータ開発を実現した。今後は、世界的な RPKI への取組も含めた標準化へのフィードバックを継続的に実施しながら、引き続き取組を継続していく。

5　査読付き誌上発表リスト

なし

6　その他の誌上発表リスト

[1]エヌ・ティ・ティ・コミュニケーションズ株式会社 ＣＳＲ報告書 2009、インターネット経路制御の高信頼化

7　口頭発表リスト

[1]吉田友哉、“IRRを用いた次世代BGP経路制御アーキテクチャーの提案”、TM・IN・OIS 研究会（別府市）（2007年1月18日）

[2]水口孝則、吉田友哉、“Inter-Domain Routing Security ~BGP Route Hijacking~”、APRICOT 2007（ジャカルタ）（2007 年 3 月 1 日）

[3]宮川晋、水口孝則、吉田友哉、“Inter-Domain Routing Security ~BGP Route Hijacking~”、Juniper Networks Private Forum 2007（東京）（2007 年 8 月 31 日）

[4]白崎泰弘、吉田友哉、“High Availability Software”、RIPE55DataBaseWG(アムステルダム)（2007 年 10 月 26 日）

[5]白崎泰弘、吉田友哉、“High Availability Software Update for IRR”、RIPE56DataBaseWG（ベルリン）（2008 年 5 月 8 日）

[6]宮川晋、“経路ハイジャック検知・回復・予防技術の開発と実用化”、インタロップ 2008（幕張）（2008 年 6 月 11 日）

[7]吉田友哉、“ルーティング最前線”、JANOG23（高知）（2009 年 1 月 22 日）

[8]吉田友哉、“Inter-domain Routing Security~Prevention of BGP Route Hijacking~”、Asia Pacific J-Tech Forum 2009（北京）（2009 年 9 月 1 日）

[9]宮川晋、“Upcoming Technologies and New Future ISP Business”、NTT Communications lnternet Business Forum Hong Kong 2009（香港）（2009 年 12 月 3 日）

[10]宮川晋、“インターネット経路ハイジャックの検知。回復・予防についてーあなたのネットワークは乗っ取られていませんか?ー”、Global IP Business Exchange2010（東京）（2010年2月23日）

[11]田原光穂、大島利充、草場律、馬島宗平、田島悟志、川村宜伯、成田亮介“経路ハイジャックに伴う通信障害の回復方式の検討”、TM 研究会（宮古島）（2007 年 3 月 16 日）

[12]田原光穂、大島利充、草場律、馬島宗平、“経路ハイジャックに対する被害 AS による暫定処置方式の検討”、電子情報通信学会 2007 年総合大会（名古屋）（2007 年 3 月 22 日）

[13]大島利充、田原光穂、草場律、馬島宗平、田島悟志、川村宜伯、成田亮介“A Study of Recovering from Communication Failure Caused by Route Hijacking”、APNOMS 2007（札幌）（2007 年 10 月 12 日）

[14]田原光穂、大島利充、馬島宗平、“経路ハイジャックに対する通信回復時における経路制御法の検討”、電子情報通信学会 2007 年ソサイエティ大会（鳥取）（2007 年 9 月 12 日）

[15]田原光穂、大島利充、老松敏雄、馬島宗平、“導通試験を用いた経路ハイジャック判定方法の検討”、電子情報通信学会 TM 研究会（石垣）（2008 年 3 月 14 日）

[16]田原光穂、大島利充、老松敏雄、馬島宗平、“重要経路監視方式の検討”、電子情報通信学会 2008 年総合大会（北九州）（2008 年 3 月 19 日）
[17]田原光穂、“A Method to Detect Prefix Hijacking by Using Ping Tests”、APNOMS 2008 （北京）（2008 年 10 月 24 日）
[18]田原光穂、“オリジン AS 詐称経路ハイジャックの検出方式の検討”、電子情報通信学会 2009 年総合大会（松山）（2009 年 3 月 19 日）
[19]田原光穂、“AS パス詐称経路ハイジャックの検出方式の検討”、電子情報通信学会 ICM 研究会（奄美）（2009 年 3 月 12 日）
[20]瀬戸三郎、“Detecting and Recovering Prefix Hijacking using Multi-Agent inter-AS Diagnostic System、NOMS 2010（大阪）（2010 年 4 月 21 日）

8　出願特許リスト

[1]日本電信電話株式会社、ルータ、経路制御方法および経路制御プログラム、日本、2007 年 8 月 17 日
[2]日本電信電話株式会社、経路ハイジャック検出方法、経路監視装置、経路ハイジャック検出システムおよび経路ハイジャック検出プログラム、日本、2007 年 11 月 6 日
[3] 日本電信電話株式会社、経路監視装置、経路監視プログラムおよび経路ハイジャック検出システム並びに経路ハイジャック検出方法、日本、2009 年 2 月 27 日

9　取得特許リスト

[1]日本電信電話株式会社、経路情報生成広告方法、経路情報生成広告装置および経路情報生成広告プログラム、日本、2007 年 2 月 28 日、2009 年 8 月 28 日、特許 04365868
[2]日本電信電話株式会社、経路情報変更方法、経路情報変更装置および経路情報変更プログラム、日本、2007 年 2 月 28 日、2009 年 8 月 28 日、特許 04365869

１０　国際標準提案リスト

なし

１１　参加国際標準会議リスト

なし

１２　受賞リスト

なし

１３　報道発表リスト

[1] “インターネット経路情報データベースの高信頼化に向けた実証実験の開始について-NTT Com Field Tests Advanced IRR for Reliability and Security-”、NTT コミュニケーションズ株式会社ニュースリリース、2009 年 2 月 20 日
[2]“経路ハイジャックの予防を実現するインターネット接続事業者向けルータの新技術開発について”、NTT コミュニケーションズ株式会社ニュースリリース、2009 年 5 月 27 日

研究開発による成果数

	平成 18 年度	平成 19 年度	平成 20 年度	平成 21 年度
査読付き誌上発表数	件（　件）	件（　件）	件（　件）	件（　件）
その他の誌上発表数	件（　件）	件（　件）	件（　件）	１件（　件）
口　頭　発　表　数	４件（１件）	６件（３件）	６件（２件）	４件（２件）
特　許　出　願　数	２件（　件）	２件（　件）	１件（　件）	件（　件）
特　許　取　得　数	件（　件）	件（　件）	件（　件）	２件（　件）
国際標準提案数	件（　件）	件（　件）	件（　件）	件（　件）
国際標準獲得数	件（　件）	件（　件）	件（　件）	件（　件）
受　　賞　　数	件（　件）	件（　件）	件（　件）	件（　件）
報　道　発　表　数	件（　件）	件（　件）	１件（１件）	１件（　件）

	合計	（参考） 提案時目標数
査読付き誌上発表数	件（　件）	１件（　件）
その他の誌上発表数	１件（　件）	件（　件）
口　頭　発　表　数	２０件（８件）	１１件（　件）
特　許　出　願　数	５件（　件）	２件（　件）
特　許　取　得　数	２件（　件）	２件（　件）
国際標準提案数	件（　件）	件（　件）
国際標準獲得数	件（　件）	件（　件）
受　　賞　　数	件（　件）	件（　件）
報　道　発　表　数	２件（１件）	２件（　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。