平成24年度「通信プロトコルとその実装の安全性評価に関する研究開発」（副題：インターネットにおける隠蔽通信路の生成・検知・対策手法に関する研究開発）の研究開発目標・成果と今後の研究計画

1. 実施機関・研究開発期間・研究開発費

◆実施機関　　慶應義塾大学
◆研究開発期間　　平成22年度から平成24年度（3年間）
◆研究開発費　　総額98．7百万円（平成24年度　30．9百万円）

2. 研究開発の目標

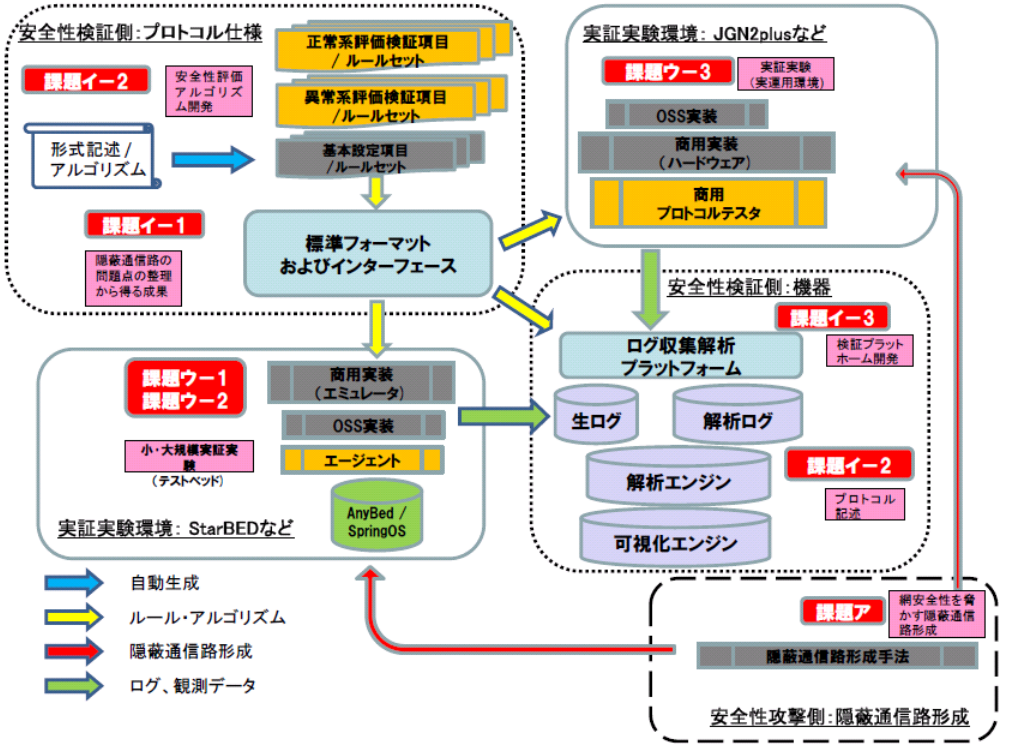
本研究開発では、隠蔽通信路を活用した情報漏洩等の防止に役立つ方法論を確立する。

従来の研究活動で対象としていた、インターネットにおける経路制御プロトコルである BGP の属性を用いた手法に限定せず、隠蔽通信路の構成法に関する検討を行う。隠蔽通信路の生成手法に対して、発覚しにくい条件での“実用的”通信容量といった具体的な検討も行う。

・通信プロトコルとその実装の安全性評価に関する研究開発課題と担当
担当：慶應義塾大学
課題ア　インターネットにおける隠蔽通信路構築手法の研究開発
課題イ　インターネットにおける隠蔽通信路に対する安全性評価アルゴリズムの研究開発
課題ウ　隠蔽通信路に対する安全性評価手法に関する検証実験

3. 研究開発の成果

「通信プロトコルとその実装の安全性評価に関する研究開発」の主な成果



研究開発の全体イメージ図

課題ア－1 隠蔽通信路の構築手法の検討と事前評価

■目標

整理した隠蔽通信路の分類、通信モデル、脅威モデルを踏まえ、脅威モデルと対策手法の分類の詳細化を行い、評価メトリックの定義を実施し、それを文書化する。

■成果

・既存の隠蔽通信路分類手法，構築手法，対策手法に関して調査し，調査した結果をサーベイ論文としてまとめた。
・平成23年度に作成した通信モデルを用いた分類手法の整理で得た知見をもとに，評価メトリックおよび対策手法反映に関する指針をまとめた。

「通信プロトコルとその実装の安全性評価に関する研究開発」の主な成果

ア－2 隠蔽通信路の実装

■目標

設計したスイッチによる隠蔽通信路構築手法の実装する。また、可能性を明らかにしたBGP経路ハイジャックを利用した隠蔽通信路に対して、実験を行うために必要な設定方法の洗い出しを行う。

■成果

・BGP オプションおよびBGP経路ハイジャックによる隠蔽通信路構築の実験を行うために必要な設定方法を洗い出し、実験環境構築ツールとしてまとめた.
・他，OSPF，IP オプション，TCP再送制御，スイッチングハブによる隠蔽通信路の実装を行い、容易に実装可能であることがわかった。

ア－3 隠蔽通信路の実際的な評価

■目標

実装したTCP Reply 攻撃を応用した隠蔽通信路に関し、検証サーバに対するウェブアクセスと確認ツールを用いて検証を行う。またiBGPにおける隠蔽通信路、およびeBGPにおける経路ハイジャックを用いた隠蔽通信路ア－2で実装された隠蔽通信路について、StarBEDを使った再現実験を実施し、評価する。

■成果

・IPオプション，TCP再送制御，スイッチングハブに関しては実環境において検証を行い，その利用可能性を検証した。検証結果から、制限はあるものの、一般的なインターネット接続環境で利用できることがわかった。
・BGPに関してはStarBEDを利用した模擬インターネット環境にて検証を行い，経路ハイジャックを容易に再現できることを確認した.

イ－1 隠蔽通信路に対する評価項目、評価ルールに関する標準フォーマットの開発

■目標

開発した形式モデルによる簡単なネットワークプロトコルの検証と評価を行う。検証、評価においては、形式モデルの専門家の意見を仰ぐ。

■成果

・FPGAによるハードウェアサポートを用いたより柔軟なテスタ作成フレームワークとして，EtherPIPEを開発し，オープンソースとして公開した．EtherPIPEによってOSの標準入出力を用いて柔軟にテスタを作成できるようになった。
・形式モデルの専門家との協議の結果，仕様書から状態遷移機械を作成し，その状態遷移機械に対して実際のネットワークトラフィックから統計的標準モデルを作成し，ネットワーク機器の挙動に対する検証ルールをモデルチェックツールにより自動生成する検証手法を提案した。提案手法により、検知ルールセット作成の自動化に関する可能性を示した。

イ－2 隠蔽通信路に対する安全性評価ルールセット生成アルゴリズムの開発

■目標

開発した安全性検証フレームワークのプロトタイプ実装を評価する。また、設計した安全性検証フレームワークに関し、国内外の研究会にて発表し、研究者らからの忌憚のない意見を収集し、プロトタイプ実装の改修に反映する。

■成果

・課題イ－1で提案した形式モデルによる検証手法の適用例としてOSPFv2を対象に標準モデルを作成した。これにより複雑なルーティングプロトコルに対しても形式手法を適用できることが明らかとなった，また、作成したモデルは国内研究会にて発表し，研究者らからの忌憚のない意見を収集し、課題を明らかにした 。
・OSPFv2の標準統計モデルを作成するためにStarBED上に構築した疑似OSPFバックボーン環境を用いてデータセットを取得した。データセットの解析を試みたが、信頼性のある標準統計モデルを作成することは非常に難しいことが明らかとなった。

「通信プロトコルとその実装の安全性評価に関する研究開発」の主な成果

イ－3 隠蔽通信路検証に必要なログ収集解析プラットフォームの開発

■目標

開発した収集ログの解析が実施できるログ収集解析プラットフォームを用い課題ウと連携して実験を実施する。また、課題イ－3にて開発された検証フレームワークと組み合わせた利用をまとめ、改修を行う。

■成果

・FreeBSD JAILを用いたソフトウェアルータ・ハードウェアルータの隠蔽通信路可能性を検証する挟み込み型検証フレームワークCovertJAIL を改修し，OSPFモデル化を行う上で必要となるOSPF向け情報収集probe をモジュールとして作成し，実験を行った。行った改修により、実験の省力化が実現できた。

ウ－1 小規模実験環境における安全性評価手法の開発と検証実験

■目標

課題ア、課題イの各課題で開発された安全性評価手法を通信機器単体、または複数の通信機器、あるいはソフトウェア実装をもとにした小規模な実験環境での隠蔽通信路構築手法および安全性評価検証実験手法の検証と改修を実施する。また、課題ア-3 で実施される隠蔽通信路生成手法の評価および、課題イ－2の検証フレームワークで生成されたルールセットをもとに課題イ－3で開発されるログ収集機構をもとに安全性検証実験環境の構築を行うための実験フレームワークおよびツールセットの検証と改修を行う。

■成果

・CovertJAILを用い商用ルータに対する安全性検証を行う小規模実験環境を構築し検証 を実施した．検証結果から、実験の省力化が実現でき、先行研究で指摘された隠蔽通信路構築への対策が実装されていることを確認できた。
・課題ア－3と連携し経路ハイジャック構築実験を実施・検証し、容易に検証環境を構築できることを示した。

ウ－2 大規模実験環境における安全性評価手法の開発と実証実験

■目標

課題ウ－1で開発された実験手法を大規模実験環境での並列実験や規模拡大実験を可能にする実験手法の検証と改修を実施する。

具体的には、StarBED などの大規模検証施設上に、小規模実験環境と同等のソフトウェアのみで構築した検証環境を構築し、これを並列実行して安全性検証を実施するための並列化フレームワークおよびツールセットの検証と改修を行う。

■成果

・CovertJAIL の並列実行を検証し，シナリオに従って並列化して 検証できることを確認し、大規模並列実験の省力化を実現した。
・FAI(Fully Automatic Installation) を使ったインストール手法の 開発し，並列化実験のための初期セットアップ・イメージ複製の 時間短縮を実現 した。

ウ－3実運用環境における安全性評価手法の開発と実証実験

■目標

課題ウ－2に置いて開発される小規模実験環境、大規模実験環境における実験フレームワークをもとにして、実環境において同様の実験フレームワークで検証を実施する際の課題や問題点、必要となるツールセットや運用方法などに関して検討し、検討結果を文書化する。

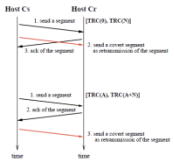
■成果

・StarBED上へのWIDEバックボーン疑似環境を構築し，OSPFv2 統計モデル作成のためのデータセットを取得した 。これにより、テストベッドにおける実インターネットの疑似環境構築に関する知見を得た。
・TCP 再送を用いた隠蔽通信路を実環境下で検証し，透過性やログ出力を検証した 。これによりTCP 再送を用いた隠蔽通信路の実用性が明らかとなった。
・バックボーンネットワークにおいて，S-Transform などのデータマイニング手法をDNSトラフィックに適用し，運用ツールとして利用するための改善点を文書としてまとめた．これにより、運用上扱えるデータマイニング手法を応用した検知手法の開発が必要であるとの知見を得た。

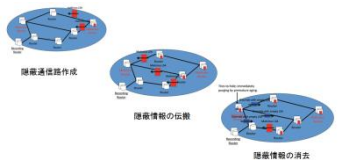
「通信プロトコルとその実装の安全性検証に関する研究開発」での3年間の研究開発成果概要

①インターネットにおける隠蔽通信路構築手法の研究開発

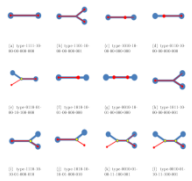
・300本以上の文献調査から隠蔽通信路を構築する特徴を抽出し，通信モデルによる分類など，新しい分類手法を2種類構築した。
・実用性（潜在的脅威）の高い隠蔽通信路構築手法を6種類実装した。
・実環境で検証可能な手法2種類に関して実環境で実施し，それ以外はインターネット環境を模した疑似環境上で特性評価を実施し、知見を得た。
・対策手法が存在し，公開しても問題のないと考えられる隠蔽通信路構築手法に関しては文書化し，研究論文や収録論文，標準化草案として発表し、コミュニティに寄与した.



=TCP再送偽装隠蔽通信路=

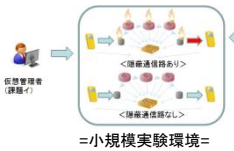


=OSPF における痕跡消去型隠蔽通信路=


=通信モデルによる系統的な分類=

③隠蔽通信路に対する安全性評価手法に関する検証実験

・検証フレームワークCovertJAILおよびAnyBedを用いた小規模実験環境構築手法を構築し、検証の省力化に寄与した。
・小規模実験環境の並列化，大規模化手法を構築し、検証の省力化に寄与した。
・危険性の少ない2種類の隠蔽通信路構築手法対し実環境下での安全性検証を実施し、実インターネット上での隠蔽通信路構築に関する知見を得た。
・危険性の高い3種類の隠蔽通信路構築手法に関し，StarBED上に構築したインターネット模擬環境下で特性評価を実施し、模擬環境を用いた実験手法の有効性評価に寄与した。



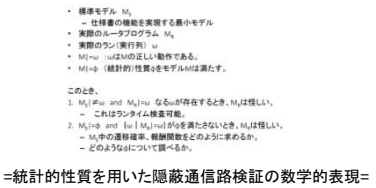
=小規模実験環境=

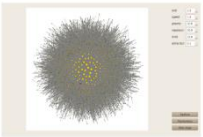
=実インターネット環境・模擬インターネット環境=
=大規模実験環境=

②インターネットにおける隠蔽通信路に対する安全性評価アルゴリズムの研究開発

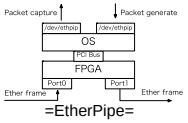
・IETF OPSEC 分科会での標準化草案にもとづいた安全性評価ルールの試作し、試作したルールセットで異常なパケットを効率的に計測できることが分かった。
・XSDを用いた標準メッセージフォーマットITBBAssessment.xsdとAPIの試作し、連携例を示した。
・ハードウェア化における開発フレームワークMagukaraとハードウェアをOS上のキャラクタデバイスとして提供するインターフェースであるEtherPipe を開発し、より柔軟なテスタ開発に寄与した。
・標準モデルの統計的性質の差異を用いたランタイム検証によるルーティングプロトコル安全性検証手法を試作し、検証ルールセット生成自動化の可能性を示した。
・並列実験向けログ収集・解析フレームワークCovertJAILを開発し、実験省力化に寄与した。
・リアルタイム実験向けログ収集・解析・可視化フレームワークBGPViewを開発した。本研究以外での大規模実験の可視化に応用され、ツールとしての有用性を示した。


=ITBBAssessment.xsd=


=統計的性質を用いた隠蔽通信路検証の数学的表現=

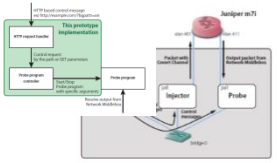

=BGPView=


=Magukara=



=EtherPipe=


=OSPFv2 に関する標準モデル=



=CovertJAIL=

4. これまで得られた研究成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	報道発表	展示会	標準化提案
通信プロトコルとその実装の安全性評価に関する研究開発	0 （0）	0 （0）	3 （2※）	6 （2※）	0 （0）	0 （0）	2 （0）

※ 現在，課題ア－1 隠蔽通信路分類手法を論文誌に，課題ア-2 EtherPIPEを国際会議に投稿中，査読結果待ち

※成果数は累計件数と（ ）内の当該年度件数です。

5. 展示会、研究成果発表など

（1）展示会 ： 特になし

（2）研究成果の学会・会議発表

- 室田朋樹, 櫨山寛章, 加藤朗. 形式化アプローチによるルーティングプロトコルの安全性検証. 電子情報通信学会 技術研究報告, vol. 112, no. 430, IA2012-86, pp. 95-100, 2013年 2月.
- 空閑洋平, 松谷健史, 櫨山寛章, 中村修. FPGAを用いた柔軟なネットワーク試験環境の実現. 電子情報通信学会 技術研究報告, vol. 112, no. 430, IA2012-85, pp. 89-94, 2013年 2月.（学生奨励賞受賞）

6. 今後の研究開発計画

・文書化した隠蔽通信路研究の最新動向やEtherPIPE などは研究論文等で発表していく.
・また，一般に啓蒙するために、解説記事やオペレータコミュニティでの発表を検討していく.
・情報通信研究機構セキュリティアーキテクチャ研究所と連携し，本研究で得た成果の発展研究を検討していく。