平成23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」の開発成果について

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23年度　32．9百万円）

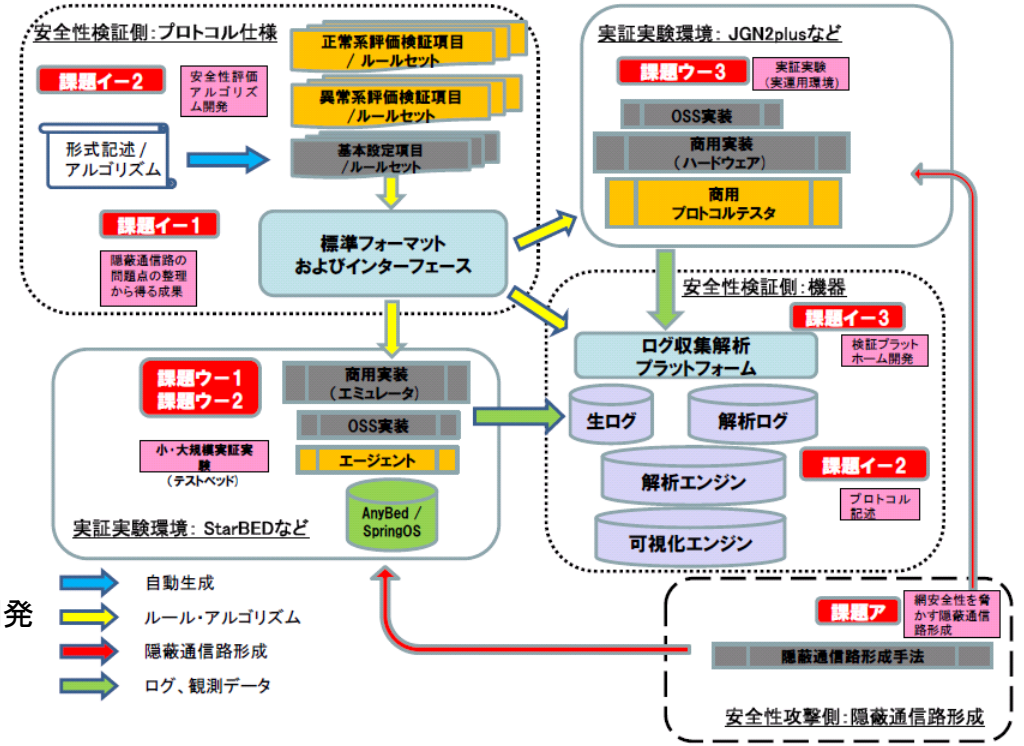
2. 研究開発の目標

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検証プラットフォームの研究開発
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

H22年度に検討した隠蔽通信路に関する構築方法の具体的な検討。実インターネットでの隠蔽通信路に利用されやすいプロトコルの利用状況の調査および文書化。

■成果

・OSPF、TCP Reply、スイッチによる中間者攻撃、IPオプション利用、BGP経路ハイジャックを用いた隠蔽通信路の構築手法に関して具体的に検討を実施した。
・OSPF を隠蔽通信路構築手法に関しては防御手法とともに標準化草案を作成し、第81回IETF標準化会議OSPF分科会にて発表(2011年7月)した。
・隠蔽通信路を通信モデルの視点から分類し、国内査読付き会議（IC2011）にて発表(2011年10月)した。また、最新事例を加筆し国内論文誌に投稿し査読を受けている。
・IPオプション付きパケットの透過性検証を実施し、APAN meeting Chen Mai にて口頭発表(2012年2月)を行った。現在、予稿集採録のための査読を受けている。

「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

前年度(平成22年度)実施したBGPを用いた隠蔽通信路生成手法の設計について、隠蔽通信路の構築手法のプロトタイプ実装を作成し検証する。
また、そのほか実用性、危険度の高い隠蔽通信路生成手法に関して実装レベルでの設計を実施する。

■成果

- BGPAttr として実装し、課題イの検証フレームワークに組み込んだ。
- TCP Reply を用いた隠蔽通信路構築手法をFreeBSDで実装した。
- スイッチによる中間者攻撃を用いた隠蔽通信路の実装レベルでの構築方法の調査を行い、容易に実装可能であることを確認した。
- BGPの経路ハイジャックを用いた隠蔽通信路構築手法の実装を行った。

ア－3 隠蔽通信路の実際的な評価

■目標

ア－2で実装された隠蔽通信路について、実際のインターネット環境で使用することを前提にこれらの特性についての評価を行う。

■成果

- TCP Reply を用いた隠蔽通信路構築手法を検証するため、検証サーバ（http://covert.kmd.keio.ac.jp/ ）を慶應義塾大学内のネットワークに構築した。
- BGP における経路ハイジャックを用いた隠蔽通信路手法に関して評価を行った。

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

前年度(平成22年度)規定した隠蔽通信路に対する安全性評価項目および評価ルールの標準フォーマット定義について、インターネットにおける通信機器に対して隠蔽通信路生成の可能性を検証するための評価項目、および評価ルールの記述が可能かどうかの検証を実施する。
また、形式モデル化および評価項目、評価ルールの設計については、専門家の意見を仰ぐ。

■成果

- BGP、TCPに関して評価項目・評価ルールの設計を行った。
- 形式モデル化に関し専門家の意見を仰いだところ、現在の形式モデルを用いて隠蔽通信路の検証を行うことは形式モデルの仕様上、非常に困難であるが、定義をし、統計的性質を比較し異常検出することにより検証できるのではないかと指摘された。

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

平成22年度の研究結果を受け、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を包括する安全性評価フレームワークの設計とプロトタイプ実装を行う。
課題イ－1で開発される評価項目、評価ルールに関する標準フォーマットもしくは形式モデルや外部団体が定義した安全性検証ルールをもとに、課題イ－3で開発されるログ収集解析プラットフォームのモジュールへルールセットとして投入されるフィルタリングルールや入出力パケットの生成等に関して検証を行い、安全性検証フレームワークの設計とプロトタイプ開発を実施する。
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、設計や実装に反映する

■成果

- 安全性評価フレームワークのプロトタイプを実装し、課題アで開発したBGPAttr をテストモジュールとして組み込んだ
- 安全性評価フレームワークのプロトタイプを実装に関して国内研究会（IA研究会）にて発表(2012年3月)した。

「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

インターネットを構成する通信機器単体や通信機器で構成されたネットワークに対して、隠蔽通信路生成可能性への包括的な安全性検証を行うために必要となる、入出力データやログを収集し、定められた安全性評価ルールセットにより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の開発を実施する。

課題イ－2 にて生成されるフィルタリングルール、もしくは入出力パケットフォーマットを入出力モジュール、ログ収集モジュールとして組み入れられるよう、モジュールのプロトタイプ実装も行う。

■成果

- 課題イ－2の検証フレームワークのモジュールとして事後解析用にRESTプロトコルベースでログを参照できるフレームワークの設計を行った。
- BGPを用いた隠蔽通信路のリアルタイム解析用に、マルチスレッドテンプレートライブラリXDTのサンプルコードを応用したログ収集、解析ツールを開発した。

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安全性評価検証実験手法の開発を実施する。

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開発を行う。

■成果

- 経路ハイジャックを用いたBGPにおける隠蔽通信路検証環境を課題アと協力してStarBED上に構築した。
- 課題イ－3で開発したBGP実験リアルタイムログ解析の小規模環境を構築し、BGPのログをリアルタイム、事後解析できることを確認した。

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開発を実施する。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開発を行う。

■成果

- 課題イと連携し、並列化のフレームワークを設計した。
- 課題ウ－1で実施したBGP実験リアルタイムログ解析の小規模環境を1500ノード規模まで拡大し、BGPのログをリアルタイム、事後解析できることを確認した。また、従来手法で作成されていた実験の手順書を改訂した。

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－1、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

- 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を行い整理した。

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）	1 （1）	4 （3）	0 （0）	0 （0）	2 （1）

※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

（2.1） 2011年7月に、IETF 81標準化会議にて ” Consideration on OSPF LSDB Monitoring ” を発表

（2.2） 2011年10月に、インターネットコンファレンス 2011にて ”ネットワーク運用管理視点による隠蔽通信路 の分類” を発表

（2.3） 2012年2月に、32回APAN meeting にて ” Active and Passive Monitoring and Analysis of IP Option Header Transparency from Covert Channel Point of View” を発表

（2.4） 2012年3月に、IA研究会 にて ”隠蔽通信路検証フレームワークの設計と実装” を発表

6. 今後の研究開発計画

・実装を行った隠蔽通信路構築手法や対策手法を大規模実験環境や実環境にて検証を行い、隠蔽通信路としての有効性や対策手法の評価を行う。評価結果を国際会議や論文誌に投稿し発表する。