平成22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. 施策の目標

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。

2. 研究開発の背景

・現状ネットワーク機材利用への懸念(隠蔽通信路の存在) :インターネットは世界的なディジタル情報の流通基盤として用いられており、企業や政府などで活用されている。懸念として、通信において、いわば寄生した通信が考えられ、通常は用いられない方法による通信は隠蔽情報通信路(covert channel)と呼ばれ、この活用による情報流出が懸念される。

・ネットワーク機材安全性の確認の障壁:隠蔽通信路が存在しないことの確認には、機材のソフトウェアのソースコードの提供を受け、それを解析するのが一番確実である。しかし、ソースコードは機器ベンダにとっては最高機密の一つであり、その入手は困難である。隠蔽通信路が存在しないことに対する一般な証明は不可能であるが、ネットワーク機器をいわばブラックボックスと考え、外部からのメッセージのやり取りを実施・観測することによって、比較的高い確率で既に知られた機構による隠蔽通信路が存在しないことを示す方法が求められている。

3. 研究開発の概要と期待される効果

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
安全性評価に関する研究に役立てるために、隠蔽通信路の構築手法について検討を行い、いくつかの可能な隠蔽通信路について事前評価を行う。
この中で比較的“実用性”が高いいくつかの手法について実装を行い、実装も含めた評価を行う。

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
インターネットを構成するネットワーク機器に対して、通信プロトコル規格に従って隠蔽通信路に対する安全性評価ルールを生成し、安全性評価ルールに基づいた入出力の変化による検証や、観測による異常検知により隠蔽通信路に対する安全性評価を行うアルゴリズムと検証アルゴリズムに基づいた検証システムの研究開発を行う。(イ-3は来年度から実施)

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(来年度から実施)
課題アにより研究開発された隠蔽通信路生成手法と課題イにより研究開発された隠蔽通信路安全性評価システムおよび安全性評価アルゴリズムを用いた検証実験手法の確立と、確立した検証実験手法に基づいた隠蔽通信路生成、安全性評価アルゴリズムの実証実験を行う。

以上の研究開発により隠蔽通信路の安全性評価手法の確立をすることで、重要ネットワークインフラの安全性向上や商用ルータ製品の質の向上に貢献することが期待できる。

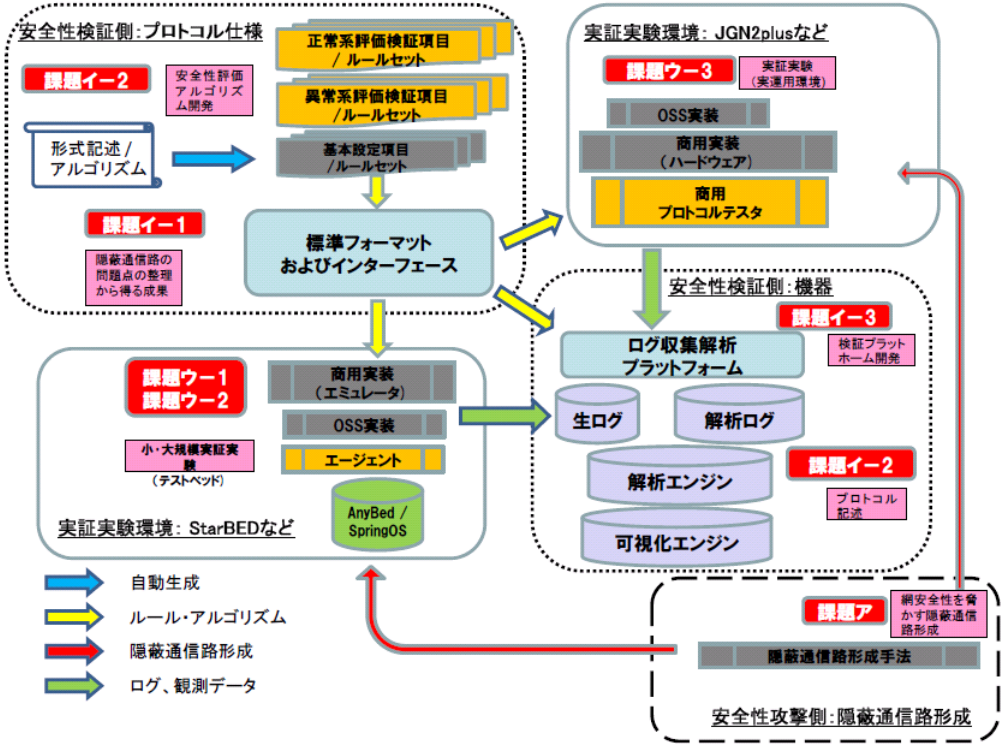

図1:研究開発の全体イメージ図

4. 研究開発の期間及び体制

平成22年度～平成24年度(3年間)
NICT委託研究(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

ア－１ 隠蔽通信路の構築手法の検討と事前評価

■目標

インターネットで常用されている通信プロトコルについて、情報を埋め込むことができる余地について検討し、隠蔽通信路を生成できる可能性のある通信プロトコルを調査し、構築法を系統的に分析する。

■成果

隠蔽通信路の構築手法と対策手法に関する過去の研究や本プロジェクトで着目している中間ノードによる隠蔽通信路構築や対策手法の現状および、隠蔽通信路構築手法に関する分類指標をまとめ、構築方法を系統的に分析するという当初の目標を達成した。構築法の系統的な分析結果は電子情報通信学会ICSS研究会にて発表した。表1の記号はICSS 研究会「インターネットにおける隠蔽通信路の可能性とその検証についての一考察」に記載した分類指標に対応して隠蔽通信路構築手法の特徴づけを行った表である。

	Payload Encoding	# of Recv.	Specify of Recv.	Type of Recv.	Location of Recv.	Location of Sender	Type of Sender	Transfer Manner	Intention	Methods	Injection Timing	Layer	Dist. Manner	備考
L2	z	単数	特定	z	z	z	中間ノード	Hop by Hop	Close	Storage	z	z	Unicast	
BGP	z	複数	不特定	中間ノード	中間	中間	中間ノード	End to End	Open	Storage	z	L3	Multicast	
DNStunnel	あり	単数	特定	中間ノード・TAP	末端	末端	末端ノード	End to End	Close	カプセル化	z	L7	Unicast	
HTTPTunnel	あり	単数	特定	末端ノード	末端	末端	末端ノード	End to End	Close	カプセル化	z	L7	Unicast	
ICMPtunnel	あり	単数	特定	末端ノード	末端	末端	末端ノード	End to End	Close	カプセル化	z	L4	Unicast	
暗号化通信を利用したなりすまし	あり	z	特定	末端ノード	末端	末端	中間ノード	End to End	Close	暗号路	z	L7	Unicast	
タイミングチャネル	z	z	z	z	z	z	z	z	z	Timing	z	z	z	
未使用ビットの不正利用などヘッダへの埋め込み	z	z	z	末端ノード	z	z	z	z	Close	Storage	z	z	z	
パディングの不正利用	z	z	z	末端ノード	z	z	z	z	Close	Storage	z	z	z	
パケットロス、フレーム衝突タイミングへの埋め込み	z	z	z	z	z	z	z	z	z	Timing	z	z	z	
BackDoor	z	z	z	z	z	z	z	z	Close	z	Pre-installed	z	z	一般的な Backdoor
Remote Exploit	z	z	z	z	z	z	z	z	z	z	Exploit	z	z	一般的なリモート Exploit
Lawful Intercept攻撃	z	z	z	z	z	z	中間ノード	z	z	z	Pre-installed Explout	z	z	ネットワーク機器の通信傍受機能に対する Exploit

表1：分類指標を用いた隠蔽通信路構築手法の特徴づけ
（特定パターンに分類できない特徴はz で表記）

ア－2 隠蔽通信路の実装

■目標

過去の研究から隠蔽通信路生成可能性が指摘されているBGPに関し、PCルータにて実装可能か否かを検証し、BGPを用いた隠蔽通信路生成手法の設計を行う。

■成果

BGP は経路に属性を付して経路情報の公告を行い、属性を評価して経路選択を可能にするプロトコルであり、将来の拡張に対応するため、未定義属性に関し て、図2のような属性のフラグによって当該属性を廃棄するか、未解釈のまま 転送するかの指示が可能である。未定義属性を用いた隠蔽通信路に関して、4K バイト程度のメッセージの伝搬が可能であり、いくつかのルータではこれらが 通常のコマンドでは表示されないことを確認した。また、Perlを用いた簡易スクリプトを作成し、PCルータにて実装可能か否かの検証も実施し、当初の目標を達成している。この他、既知の属性を用いた隠蔽通信路についての検討や、OSPF による隠蔽通信路構築手法やその検出についての検討も行った。

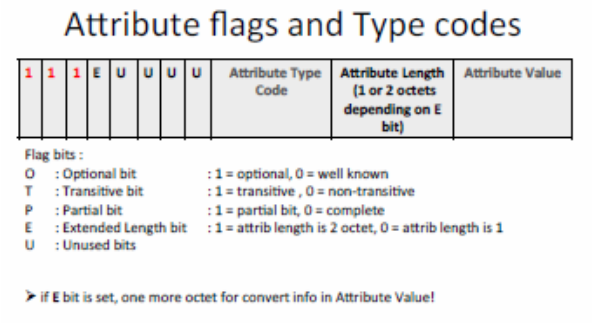

図2：BGPを用いた隠蔽通信路の設計

ア－3 隠蔽通信路の実際的な評価

ア－3 隠蔽通信路の実際的な評価については、来年度から実施。

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

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

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、および評価ルールが記述可能な標準フォーマットを開発（含むAPI）する。

隠蔽通信路に対する安全性評価項目および評価ルールを記述するためのXSDやRDFなどのマークアップ言語定義を用いて標準フォーマット定義を規定する。また、課題イ－2、課題イ－3の実装から容易に標準フォーマット定義に基づいたメッセージを出力できるためのAPIもしくはモジュールを提供する。

■成果

形式モデル記述やAFM（Automated Formal Methods）、APTG（Automatic Test Pattern Generation）などネットワークプロトコルのモデル検証、ソースコード検証に関する先行研究の調査やIPヘッダ、IPオプションに絞り込んで隠蔽通信路に関する入出力テストパターンや検知フィルタルールの策定を実施した。また、IPヘッダおよびIPオプションに関するテストパターン、フィルタルールをもとにXSDにて標準フォーマットを仮定義し、XML::PastorによってAPIを作成した。

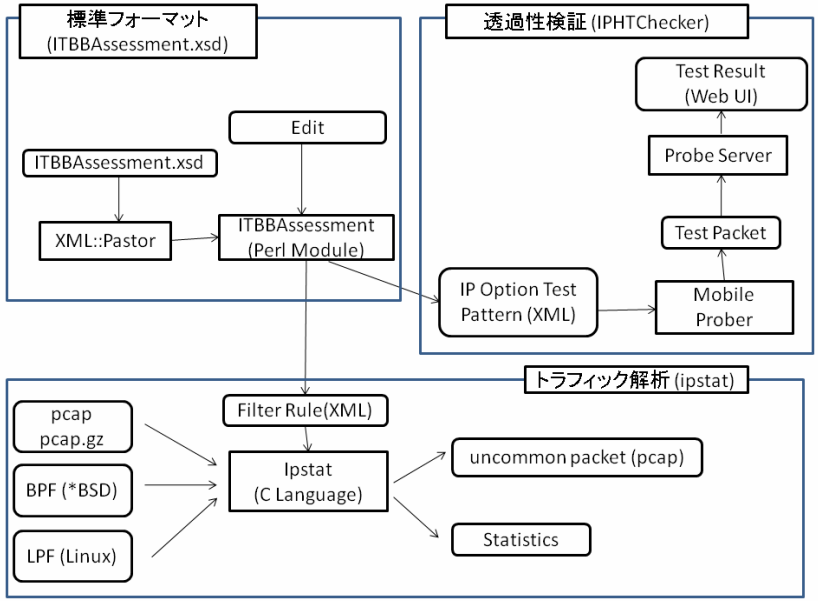

図3：標準フォーマットと試作した検証ツール

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

通信プロトコル規格からその通信プロトコルの隠蔽通信路生成可能性に対する安全性評価を行うための評価ルールセット、通信プロトコル記述フレームワークおよび安全性評価ルールセット生成アルゴリズムの設計を行う。

■成果

形式モデル記述の専門家を交え、形式モデルを用いた検証手法とネットワークプロトコルの検証に関する応用研究や、ソフトウェアソースコードからのテストパターン自動生成に関する最新研究に関する調査を実施し、分析、分類を行った。また、形式モデル検証とソースコード検証を統合的に扱うためのフレームワークの設計を行い、目標を達成した。ルールセット生成アルゴリズムに関しては形式モデル記述の専門家からの助言により、より詳細な調査や具体的なモデル化を通して設計するのが好ましいという結果になり、平成23年度以降に詳細な設計を実施することにした。

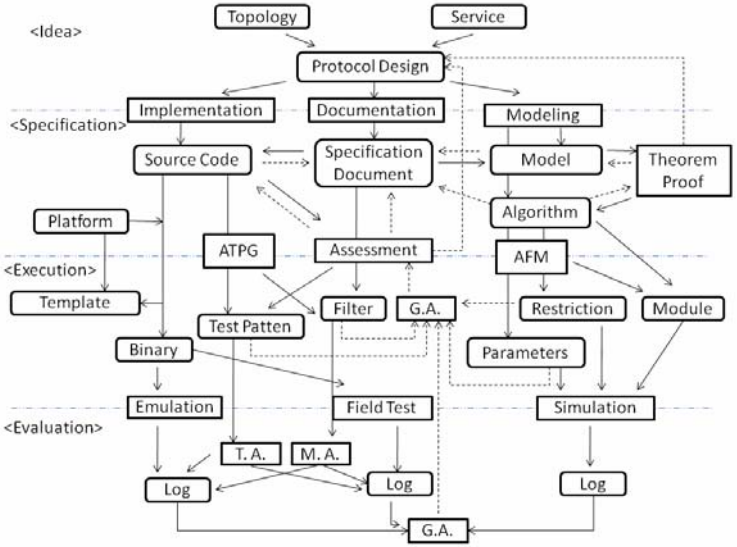

図4：プロトコル安全性検証フレームワーク

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

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については、来年度から実施する。

1．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	1	0	0	0

（1）表彰・受賞

・とくになし

（2）研究成果の学会・会議発表

・電子情報通信学会 ICSS 研究会（3月25日）、「インターネットにおける隠蔽通信路の可能性とその検証についての一考察」
※ 東日本大地震のため発表自体は中止。