3-7　ネットワークセキュリティのための再現・模倣技術

3-7 Reproducing and Emulation Technologies for Researches on Secure Networking

三輪信介
MIWA Shinsuke

要旨

ネットワークセキュリティに関する研究開発を行う上では、さまざまな攻撃についてその仕組みを解析し問題を明らかにする必要がある。また、ネットワークセキュリティに関する新しい技術が開発された場合には、それを現実に即した環境で検証する必要がある。

そこで、本稿では、ネットワークセキュリティに関する研究開発に用いるために我々が開発してきたネットワーク環境の再現・模倣技術について、その成果と応用について述べる。

Mechanisms of various attacks must be analyzed in detail for clarifying and defining targets of research and development on secure networking. Moreover, new technologies concerning secure networking must be verified on the realistic network environment.

In this paper, we describe our reproducing and emulation technologies for researches on secure networking, and its applications.

[キーワード]
再現，模倣，AS 間ネットワーク，マルウェア，封じ込め
Reproduction, Emulation, Inter-AS network, Malware, Containment

1　はじめに

ネットワークセキュリティに関する研究開発を行う上では、ウィルス・ワーム・ボットなどのマルウェア [1] やさまざまな攻撃について、その仕組みを解析し、問題を明らかにする必要がある。このような解析を行うためには、マルウェアそのものや攻撃に関わる通信内容などを集めたデータセットと、それらに基づき実際の攻撃を再現できる実験環境が必要となる。また、ネットワークセキュリティに関わる新しい技術が開発された場合には、現実に則したネットワーク環境上でその有効性や性能を検証する必要がある。

そのため、我々は、広域にわたるインターネット網から組織規模のネットワーク環境までの再現や、マルウェアや攻撃ツールを騙すための各種のサービスシステムの模倣など、ネットワークセキュリティのための再現・模倣技術の研究開発を行ってきた。本稿では、これらについてその研究背景と技術を概観し、成果と応用について述べる。

2　広域インターネットの再現・模倣技術

まず、広域インターネットにおけるネットワークセキュリティに関する実験を行うために研究開発した広域インターネットの再現・模倣技術について述べる。

2.1　背景 ― インターネットの構造

現在の ICT 環境のネットワークセキュリティを考える上では、インターネットにおけるセキュリティが中心となる。インターネットは、接続性の観点では 1 つのネットワークであるが、実際には AS（Autonomous System; 自律システム）と呼ば

れる単位で分割されており、そこに各顧客組織のネットワークが接続されている。つまり、

1）各組織のネットワーク
2）プロバイダ等の AS 内ネットワーク（Inner-AS ネットワーク）
3）AS 間のネットワーク（Inter-AS ネットワーク）

といった複数段の構造になっている（図 1）。

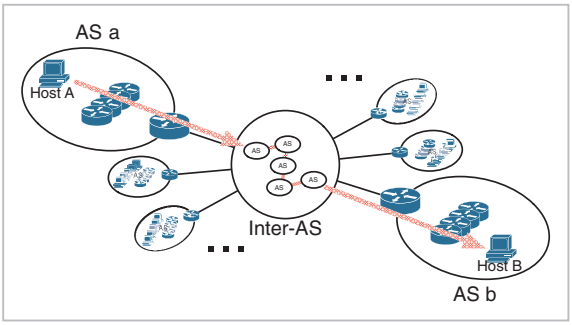

図 1 インターネットの構造

よって、インターネット上でのセキュリティ対策を導入する位置も、大別すると、

1）最終的な各ユーザの PC 等のデバイス
2）各組織ネットワークの出入口
3）AS の出入口

の 3 種類が考えられる。例えば、ウィルス対策ソフトウェアなどが 1）に、FireWall や IDS などが 2）に、経路フィルタなどが 3）に相当する。

それぞれについて新しい技術が開発された場合には、最終的にその技術を展開配備するまでには何らかの検証実験が必要となるが、その技術の展開範囲が広域になるほど、実験を行うことが困難になる。すなわち、各ユーザのデバイスや各組織のネットワークに関する技術の実験より、AS 間ネットワークに関する技術の実験は困難である。これは、実際に実験するための環境を準備する構築コストの問題と広域になることにより複数の組織の協力を必要とする運営コストの問題があるからである。

そこで、我々は特に広域にわたるインターネット上での技術に関する実験を容易にするために、AS 間ネットワークの再現・模倣技術の研究開発を行ってきた。

2.2 広域インターネットの再現・模倣手法

我々の目的は、実際にある新しい技術がソフトウェアやハードウェアとして実装された場合、その検証をなるべく現実に即した環境で行うことである。よって、広域インターネットの再現・模倣技術もいかに本物のインターネットに近い AS 間ネットワークを実験のための環境として構築するかを主要な課題とした。また、実装を対象とするため、ネットワークシミュレーターではなく、実装の試験が可能なテストベッド上に構築することが求められた。

翻って、現在のインターネットには、37,500 を超える AS がある（2011 年 5 月現在、図 2）。研究を開始した当初の 2006 年時点でも 25,000 程度であった。規模から考えると、AS 間ネットワーク全体をそのまま再現するのは困難があると考えられていたため、AS 間ネットワーク全体の再現は試みられていなかった。しかし、NICT にはおよそ 1,000 台の PC から構成されているネットワーク研究開発向けのテストベッド StarBED [2] があり、当時から仮想化技術が進展しはじめていたこととあわせて、仮想化技術と大規模なクラスタ型テストベッドの組み合わせにより、AS 間ネットワーク全体を再現・模倣するという大胆な試みを開始した。

AS 間ネットワークは、BGP（Border Gateway Protocol）によって経路制御されている。よって、AS 間ネットワークを模倣するためには BGP の

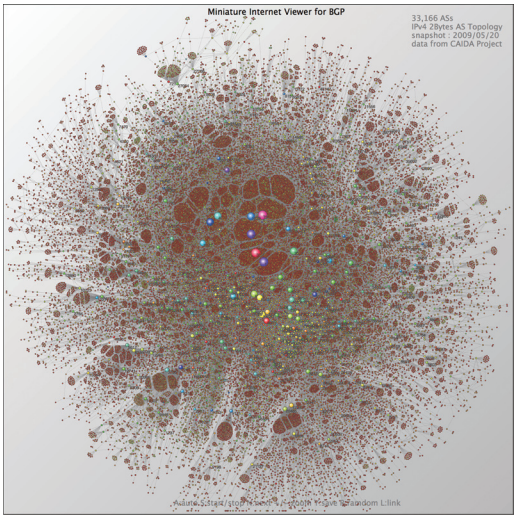

図 2 AS 間ネットワーク

ルータを必要に応じて配置する必要がある。また、AS間ネットワークは自律的に運営されているAS同士を接続方法だけを決めて接合したネットワークであり、全体の構造は管理されているわけではない。そのため、AS間ネットワークの構造を再現するためには、AS間ネットワークの構造に関する情報を観測的に手に入れることと、手に入れた情報に基づき構造を作ることが必要である。

我々は、AS間ネットワークの構造（トポロジ）データから各BGPルータの設定ファイルを自動生成するツール群（AnyBed[3]）とその設定ファイルに基づいて仮想化技術を用いてStarBEDなどのテストベッド上に大量のBGPルータを配布するツール群（XENebula[4]）を開発した。現状では、簡単のため1ASは1BGPルータとして模倣しており、BGPルーティングソフトウェアを実行できるVM（仮想機械）を大量に起動し、それらを接続することでAS間ネットワークを再現・模倣する。

AS間ネットワークの構造については、CAIDAが提供しているAS関係データセット（AS Rank annotated inferred relationship Dataset）を用いて、AnyBedで1）必要な範囲のトポロジを切り出し、2）BGPルータ間の経路を推定し、3）設定ファイルを生成する。その後、XENebulaで、その設定ファイルとテストベッド（StarBED）の資源情報を基にして、1）BGPルーティングソフトウェアが入ったVM（仮想機械）の各PCサーバへの割り当てを計算し、2）各PCサーバにそのPC上で動作するVMのOSイメージとBGPルータの設定ファイルを配布し、3）実際に各サーバ上でVMとしてBGPルータを起動する（図3）。

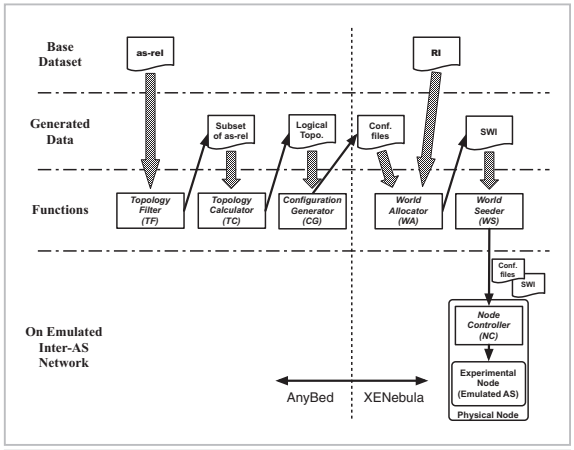

図3 AnyBed/XENebulaのアーキテクチャ

2.3 広域インターネットの再現・模倣技術の成果と応用

この手法を用いることで、実際のAS間ネットワークの3分の1に相当する10,000ASから構成されるAS間ネットワークの再現・模倣に成功している。規模の点では世界に類を見ないAS間ネットワークの再現・模倣環境であった。

実際に利用された事例として、この技術によるAS間ネットワークの再現・模倣環境を用いて、AS間IPトレースバック技術の実証実験に向けた予備実験[5]が行われた。

AS間のIPトレースバック技術はまさしく我々が想定したようなインターネット上に広域に展開される技術であり、その実証実験には複数のプロバイダにまたがる実験環境の構築と、複数のプロバイダ全体による運営が必要であるため、コストが高かった。そのため、我々が開発したAS間ネットワークの再現・模倣環境を用いて、実証実験の前に予備実験を複数回実施し、実証実験の回数や期間を最小限に留めることができたという。これは、我々が想定していた通りの成果を上げることができたといえるだろう。

AS間ネットワークの再現・模倣技術は、現在、単純に規模と構造の観点での再現・模倣を行う段階から、より速く構築することと、より正確な再現ができるようにすることを目指した研究開発が継続されている。このような大規模な再現・模倣の技術は、ネットワークセキュリティの分野に留まらず、次世代・新世代のネットワークを構築するべく研究開発が進む中で、ネットワーク技術に関するテストベッドの研究として、世界的にも1つの分野を形成しつつあり、今後の進展が期待されている。

3 マルウェア／攻撃ツールを騙すための再現・模倣技術

次に、マルウェアや攻撃ツールを騙すための再現・模倣技術について述べる。

3.1 背景 ― 隔離と再現性の対立

ウィルス・ワーム・ボットなどのマルウェアや

各種の攻撃ツールの動作やその仕組みを詳細に解析するための手法は、大きく分けて下記の2つがある。

1）プログラムコードから動作の仕組みを解析する静的解析
2）実際にそれらを動作させて観測・解析する動態解析

多くの対策技術は、マルウェアや攻撃ツールが動作したときの通信内容やファイルへのアクセス履歴などの足跡から、検知と対応を行うため、動作による影響を知ることができれば、新種のマルウェアや攻撃ツールにも対応可能となる。そのため、動作による影響を計るため、動態解析が広く用いられている。

動態解析では、何らかの実行手段で、かつ、何らかの解析環境上で、マルウェアや攻撃ツールを実際に実行し、その動作による影響を観測する必要がある。よって、マルウェアや攻撃ツールが実際に感染や攻撃などの活動を試みる。そのため、解析環境が外部に接続されている場合には、感染を拡げるなど、その影響が外部に及ぶため、何らかの対策が必要となる。また、実際のインターネット上には、非常に多くのマルウェアが蔓延しており、解析環境がインターネットに直接接続されている場合には、解析対象以外のマルウェアや攻撃の影響を受けるおそれがある。そのため、外部からの影響を排除するための何らかの対策が必要となる。

このような外部への影響や外部からの影響を排除するために、物理的もしくはネットワーク的に何らかの障壁を設けて、マルウェアや攻撃ツールの実行環境を外部と分離することを、すなわち隔離[6]が必要となる。

しかし、マルウェアや攻撃ツールには、隔離した環境での詳細な解析を避けるために、インターネット上の特定のホストやサービスへの接続性を検査して動作を変えるような解析困難化機能を備えるものが多くある。また、マルウェアや攻撃ツールが実行時にインターネットから何らかの情報をダウンロードするような場合やボットのようにネットワーク経由での命令を受けなければ動作しないものなどは、正常に動作しない。すなわち、隔離した場合には、次のような問題が生じると言える。

1）マルウェアや攻撃ツールによる実行環境の判別がし易くなる
2）マルウェアや攻撃ツールが活動するために必要な通信も阻害してしまう

よって、外部への影響や外部からの影響を避けるためには、隔離は有効な手段であるが、隔離によってマルウェアや攻撃ツールの動作が正確ではなくなり実際の動作に対する再現性の低下が起こりうるという対立がある。

そこで、我々は隔離しながらインターネット上のサービスやホストを模倣することで、マルウェアや攻撃ツールを騙し、正確な解析を目指す擬似インターネット付き隔離解析環境の研究開発を行ってきた。

3.2 擬似インターネット

マルウェアや攻撃ツールによる実行環境の判別は、自身が解析を目的とした環境で実行されていないかを検査するために行われる。その検査結果に基づいて、マルウェアや攻撃ツールは実行抑制や実体隠蔽を行い、動態解析を困難にする。

隔離対策としては、利用IPアドレスの確認や接続性の検査が行われる。利用IPアドレスの確認は、IPアドレスを検査し、隔離環境でよく用いられるプライベートアドレス空間などで動作していないかを確認する方法である。また、インターネット上の特定のホストやサービスへの接続性を検査することで、隔離環境ではないかを判別する方法がある。手法が非常に単純であるため、広く用いられている。

IPアドレスの検査に関しては、外部への影響を排除した上で、プライベートアドレス以外のアドレスを実験環境に用いればよいので、大きな問題ではない。これに対し、接続性の検査については、容易に解決することはできない。

そこで、接続性検査の対象となるサービスやホストを模倣し、接続性を誤認させる擬似インターネットを開発[7][8]することとした。

マルウェアや攻撃ツールは、基本的にソフトウェアとして何らかのPC等の実行環境上で動作する。そのため、実行環境となったPCやそのOS上で動作する機構は、すべてマルウェアや攻撃ツールに容易に検知されてしまう恐れがある。これに対し、実行環境とは違うPCやネットワーク

上で動作する機構については、マルウェアや攻撃ツールも外部観測的にしか検査することができない。擬似インターネットでは、この関係を利用し、ネットワーク上に接続性検査の対象となるサービスやホストを模倣するための VM を配置する。基本的な擬似インターネットの構成は、下記の通り。

1）有名なサイトの模倣
2）グローバルなサービスの模倣
3）ローカルなサービスの模倣
4）周辺ホストの模倣
5）経路の模倣

3.3 擬似インターネット付きマルウェア隔離解析環境

擬似インターネット付きマルウェア隔離解析環境は、仮想環境や隔離環境を判別するような解析困難化機能を持つマルウェアを安全に動態解析するための隔離解析環境である。マルウェアの解析困難化機能に対し、実ノードの切替えや再生により仮想化技術と同程度の利便性を確保する方式と擬似インターネットによりマルウェアを騙し、隔離環境で解析されていることに気づかせない方式を組み合わせて、対抗している。構成の概要を図4に示す。

再生可能な実ノードによるマルウェア実行環境である Malware Incubator と擬似インターネット機能を有する Mimetic Internet、それらを制御する制御用の Controller ノード群（以降、制御ノード群）と管理用端末からなっており、管理用端末以外はすべて隔離環境中にある。Malware Incubator 上でマルウェアを動作させ、マルウェアのインターネットへのアクセスは Mimetic Internet が模倣し、接続性検査などを騙すことができる。実験用のネットワークは物理的に分離されており、管理用のネットワークは論理的に分離されている。実行環境から管理用ネットワークへの通信は、マルウェアの実行時は完全に遮断される。実験データの収集や検体の投入を必要とする場合には、一度マルウェア実行環境を停止し、別のネットワークブートの OS で再起動した

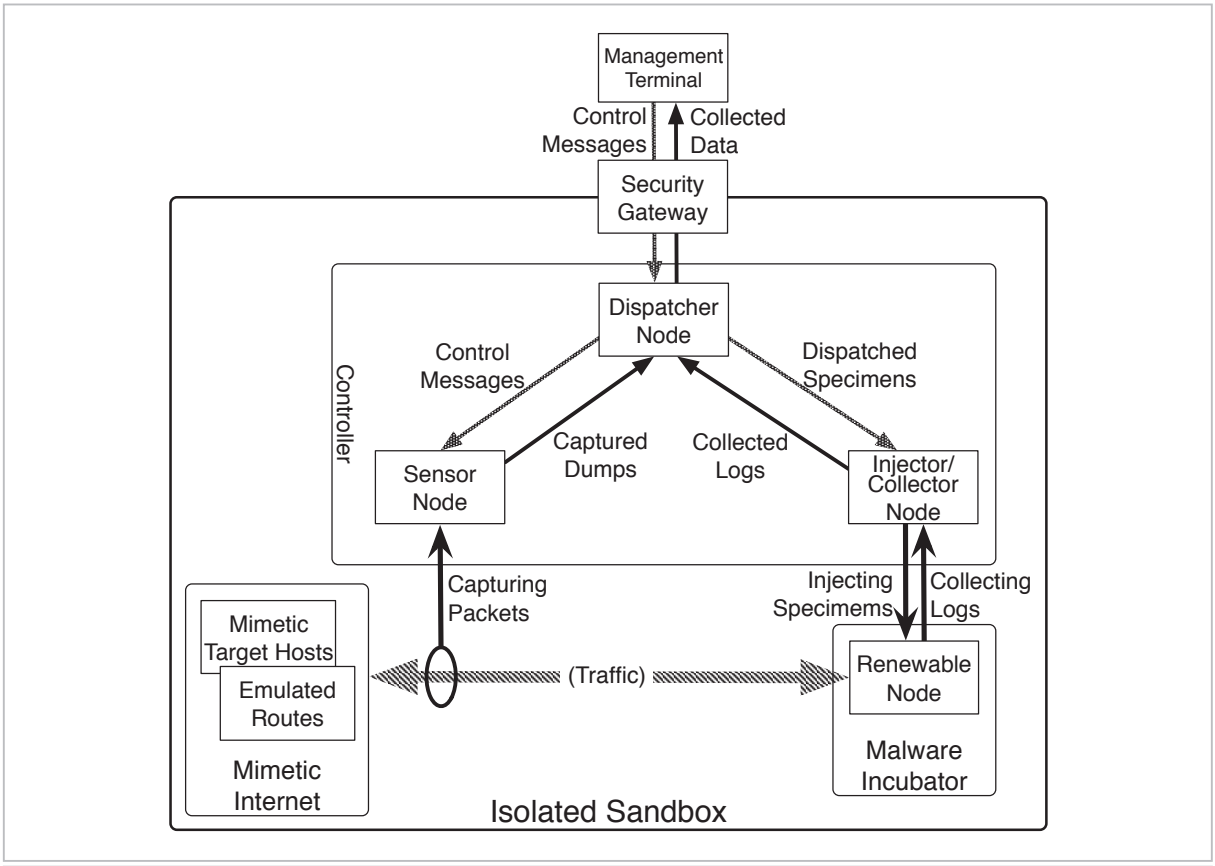

図4 擬似インターネット付きマルウェア隔離解析環境の構成

後に行うため、マルウェア活動が制御ノード群に及ぶことはない。さらに、制御ノード群と管理用端末の間には特定の通信のみを許可するSecurity Gatewayが設置され、二重に隔離を行っている。

3.4 擬似インターネットの成果と応用

擬似インターネットを有する隔離型の解析環境は、安全性と正確性の両立をはかることができる。そこで、その応用として、

1）逐次自動解析によるデータセットの生成
2）体験演習

が行われた。

逐次自動解析によるデータセットの生成では、マルウェアや攻撃ツールなどを投入すると、それを擬似インターネット付きの隔離環境内で動作させ、その際の通信内容や実行中のメモリの内容、各種のアクセスログなどを取得し、データセットとして取り出せるようにするもので、この一連の流れが自動化される（図5）。この方法によって生成されたデータセットは、実際にいくつかの学術会議において研究のための共通データセットとして採用された。

隔離環境は、危険が伴うはずの行為を安全に体験できるため、体験演習に向いている。そこで、擬似インターネット付き隔離解析環境と同じソフトウェアを用いて、StarBED上に複数の隔離環境を構築し、実際に学生がその環境を用いてマルウェアや各種の攻撃について体験しレポートを行うという「インシデント体験演習」[9]が行われた。予備を含めて15組程度の隔離環境を用いて、あらかじめ用意されているコンテンツから指定されたものを選ぶと、逐次自動解析と同様に、隔離環境内にマルウェアや攻撃ツールが投入され、実行が開始される。受講生は、隔離環境内にある監視用のサーバからその状況を監視し、どのような攻撃が行われ、どのような対策が必要かなどをレポートする。このインシデント体験演習は、2008年より3年間実施された。

擬似インターネットの技術は、現在、固定的なサービスやホストの模倣から、標的型攻撃などを

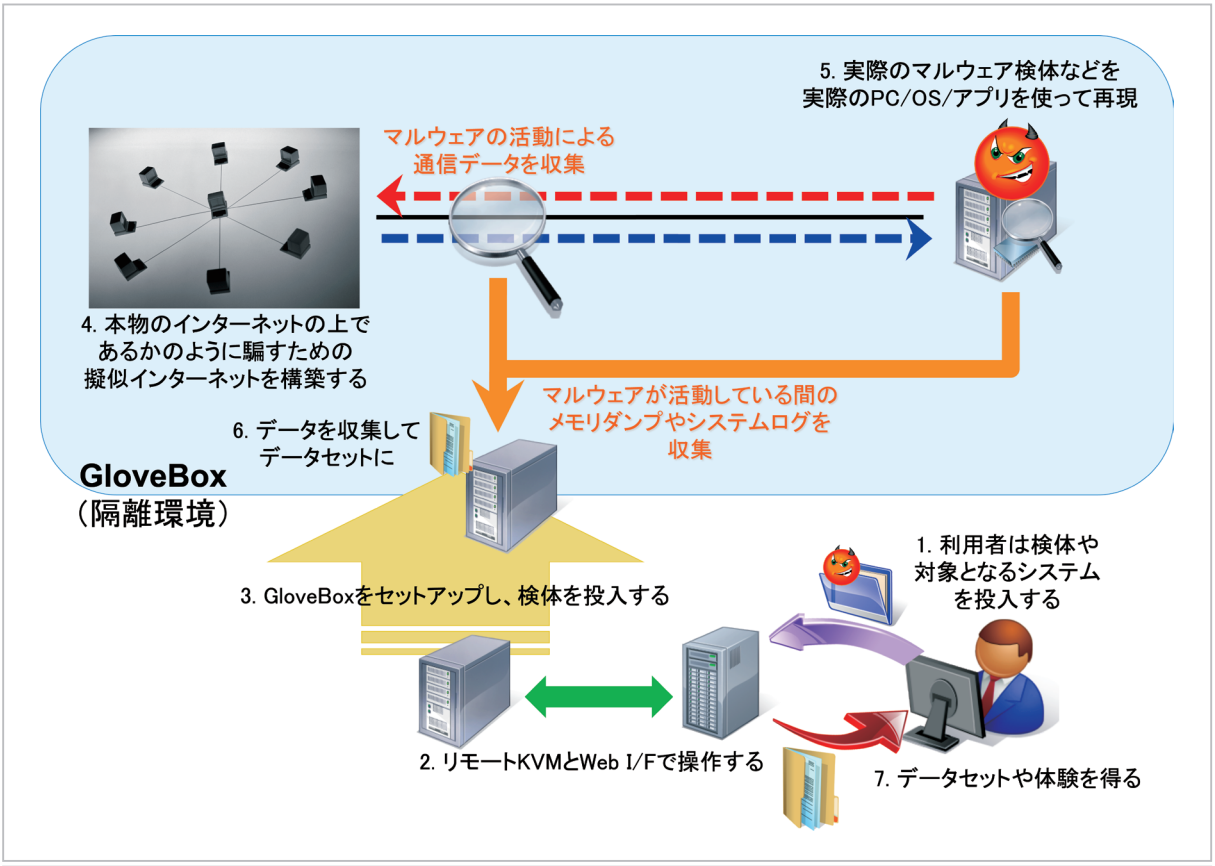

図5 逐次自動解析によるデータセット生成

対象とした自由度の高い環境の構築を可能とすること、対象となるサービスの広域なサービス網を含む正確な模倣を可能とすることを目指した研究開発が継続されている。擬似インターネットのような技術は、サービスを射影する技術であり、マルウェアや攻撃ツールを騙すためだけでなく、正確な実験を可能とするための技術として、今後の進展が期待されている。

4　課題と今後の展望

広域インターネットの再現・模倣技術も、擬似インターネットも、いずれもこれで完成したというわけではない。例えば、広域インターネットの再現・模倣では、AS間のネットワークを正確に模倣するためには、インターネットの正確な観測とそれに基づく正確な射影が必要となるが、多くの推定を含む現状では容易ではない。また、擬似インターネットにおいては、接続性検査は騙すことができるが、外部からのダウンロードや指令を必要とする場合には、それらのコンテンツも含めて擬似的に提供できなければ正確な再現・模倣はできない。さらに、再現・模倣の目指すところは、「いかに本物らしいか」の追求であるが、本物らしくすることで、本物のインターネットと同様に実験にコストやリスクがかかるようになっては、再現・模倣して構築する意味を失いかねないといった問題もある。

こういった問題を解消するためには、分散システムを別の分散システム上に射影するにはどうすればよいのか、何ができることを正確な射影（再現・模倣）と呼び、何を省いても良いのかなど、ソフトウェア科学としての研究が必要となると考えられる。このような研究が積み重ねられれば、単に解析環境や実験環境に用いるだけでなく、ICT環境全体の評価の枠組みや科学的な構成法の確立につながるなど、大きな拡がりを持つと考えられるため、進展が望まれる。

5　おわりに

ネットワークセキュリティの分野は、新しいICT環境の進展にあわせて、対象がより複雑化してきている。このような状況においては、実際に動いているソフトウェアやハードウェアと似たものを使って実験や検証を行うための技術は重要である。我々の広域インターネットの再現・模倣技術やマルウェア／攻撃ツールを騙すための再現・模倣技術は、このような実験や検証に不可欠な技術であり、実際の事例にも利用され、成果を上げている。

今後は、我々が目指した実践的な検証・実験と科学的な検証・実験とが組み合わされることで、ネットワークセキュリティが設計や開発の段階で問題を持たないことを保証できるような「セキュリティ・バイ・デザイン」が実現されることを望んでいる。

参考文献

1　E. Skoudis with L. Zeltser, “MALWARE – Fighting Malicious Code –,” Prentice Hall PTR, ISBN 0-13-101405-6, Pearson Education Inc., 2004.
2　宮地利幸，中田潤也，知念賢一，Razvan Beuran，三輪信介，岡田崇，三角真，宇多仁，芳炭将，丹康雄，中川晋一，篠田陽一，“StarBED：大規模ネットワーク実証環境，”情報処理学会，情報処理，Vol. 49, No. 1, pp. 57–70, ISSN 0447-8053, Jan. 2008.
3　Mio SUZUKI, Hiroaki HAZEYAMA, Daisuke MIYAMOTO, Shinsuke MIWA, and Youki KADOBAYASHI, “Expediting experiments across testbeds with AnyBed: a testbed-independent topology configuration system and its tool set,” IEICE Trans. of Information and System, Vol. E92-D, No. 10, pp. 1877–1887, Oct. 2009.
4　Shinsuke Miwa, Mio Suzuki, Hiroaki Hazeyama, Satoshi Uda, Toshiyuki Miyachi, Youki Kadobayashi, and Yoichi Shinoda, “Experiences in Emulating 10K AS Topology with Massive VM Multiplexing,” The First ACM SIGCOMM Workshop on Virtualized Infastructure Systems and Architectures (VISA'09), Aug. 2009.

5 櫨山寛章，若狭賢，門林雄基，“実証実験に向けたIPトレースバックシステム導入シナリオに関する一考察,”電子情報通信学会，インターネットアーキテクチャ研究会，Jul. 2008.
6 三輪信介，門林雄基，篠田陽一，“マルウェア隔離実験環境の設計と実装,”情報通信研究機構季報，Vol. 54, Nos. 2/3, pp. 15–23, 2008, ISSN 1349-3191, Sep. 2008.
7 Shinsuke MIWA, Toshiyuki MIYACHI, Masashi ETO, Masashi YOSHIZUMI, and Yoichi SHINODA,“Design Issues of an Isolated Sandbox used to Analyze Malwares,”proceedings of Second International Workshop on Security (IWSEC2007), LNCS 4752 Advances in Information and Computer Security, ISBN 978-3-540-75650-7, pp. 13–27, Oct. 2007.
8 三輪信介，宮本大輔，櫨山寛章，井上大輔，門林雄基，“模倣DNSによるマルウェア隔離解析環境の解析能向上,”サイバークリーンセンター・情報処理学会，マルウェア対策研究人材育成ワークショップ2008 (MWS2008), pp. 19–24，沖縄，Oct. 2008.
9 三輪信介，宮本大輔，櫨山寛章，樫原茂，門林雄基，篠田陽一，“インシデント体験演習環境の設計と構築,”情報処理学会，コンピュータセキュリティシンポジウム2008 (CSS2008), pp. 929–934，沖縄，Oct. 2008.

（平成23年6月15日 採録）

三輪信介（みわしんすけ）
テストベッド研究開発推進センター
テストベッド研究開発室副室長／
北陸StarBED技術センター長／
ネットワークセキュリティ研究所
セキュリティアーキテクチャ研究室主任研究員　博士（工学）
ネットワークセキュリティ