5　アプリケーション
5　Application

5-1　JGNⅡを利用した不正アクセス再現実験環境の連携実験
5-1　A Report on the Experiment of Combined Operation via JGNⅡ

三輪信介　　大野浩之
MIWA Shinsuke and OHNO Hiroyuki

要旨

インターネットセキュリティの再現実験環境では、事案に関連する各要素を実験環境内に模倣し、事案を再現することで、対策の有効性の検証や影響の計測を行うことができなければならない。しかし、インターネット上のセキュリティ事案は、規模拡大と複数事象の併発や相互干渉のため近年複雑化しており、再現実験環境は種類に応じて得手不得手があるため、単一実験環境での再現は困難となってきている。

そこで、我々は、既に存在している実験環境同士を接続し、連携させることで、コストを最小限に抑え、規模の拡大や再現対象の複雑化に対応することを検討する。

本稿では、このような実験環境の連携について検討するために、実際に我々が今まで研究開発してきたSIOS、VM Nebula、StarBEDの三つの実験環境をJGNⅡを利用して接続した連携実験について、特に接続に関する評価を述べる。

To analyze security incidents and verify security measures, an environment is required that enables the user to track and analyze phenomena caused by attacks, while taking the interaction among systems into consideration. However, security incidents have recently been growing more and more complex due to an increase in scale, simultaneous incidents, or interactions among multiple events.

As a result, it is becoming increasingly difficult to reproduce security incidents within a single experimental environment. We will discuss the combined operation of existing experimental environments at minimum cost as a way to handle security incidents of increasing scale and complexity.

In this paper, we report on the connecting experiments of our reproducing environments called "SIOS", "VM Nebula" and "StarBED" via JGNⅡ.

[キーワード]
インターネット，セキュリティ，不正アクセス，再現実験，実験環境
Internet, Security, Security incident, Experimental environment, Incident reproducing

1　はじめに

インターネット上では、日々多くのセキュリティ事案が発生しており、枚挙にいとまがない。これに対し、様々なセキュリティ対策が立案され、実施されているが、新しい攻撃手法との間でイタ

チごっこが繰り返されているのが現状である。そのため、根本的な解決を図り得るような新しい対策技術が求められている。

新たな対策の策定や対策技術の開発のためには、それらの有効性と悪影響の有無などを検証する必要がある。このような目的に利用するために、我々は検証基盤となる不正アクセス等に関する再現実験環境を研究開発してきた。

再現実験環境は、その種類に応じて、再現の粒度や正確性などの再現能力と規模追従性に大きな違いがある。一般に正確な再現をできる環境ほど規模追従性に乏しく、実験環境の運用が困難であり、抽象的な再現をする環境ほど規模追従性に富み、実験環境の運用が容易である。

セキュリティ事案の多くは、OS やアプリケーションなどの実装に固有の脆弱性に基づいて引き起こされる。そのため、その原因の究明には特定の脆弱性を再現できる環境が必要となる。また、対策技術の権能や効果、影響を検証するためには、その対策技術の実装を用いたコンフォーマンステストが必要となる。同時に、近年セキュリティ事案の影響範囲は拡大しており、さらに対策技術も広範囲に適用することを前提としたものが登場しているため、これらの分析・検証には、大規模な実験環境が必要となる。

このように、セキュリティに関する実験環境では、実装を用いた実験ができねばならない。すなわち、高い再現能力が要求される。しかし、セキュリティ事案の影響範囲の拡大や対策技術の適用範囲の拡大などから、規模追従性も要求されている。このような要求に対し、単一実験環境での再現は困難となってきている。

そこで、本稿では、既に存在している異なる複数の実験環境同士を接続し、連携させることで、再現能力や規模追従性の向上に伴うコストを最小限に抑え、規模の拡大や再現対象の複雑化に対応することを検討する。

このような実験環境の連携について検討するために、本稿では特に、実際に我々が今まで研究開発してきた SIOS、VM Nebula、StarBED の三つの実験環境を JGNII を利用して接続した統合実験について、特に VM Nebula と StarBED を接続した接続実験について述べる。

2 各再現実験環境の概説

まず、今回実験に利用した各再現実験環境について、概要とその特徴について述べる。

2.1 SIOS 不正アクセス再現実験装置

SIOS 不正アクセス再現実験装置[1]は、インターネットセキュリティを対象とした実機による実験環境である。これは SIOS[1] と我々が呼ぶシステムの一部である。東京都小金井市にある情報通信研究機構の小金井本部に設置されている。

不正アクセス再現実験装置は、100 台の PC からなる DDoS 攻撃再現部と帯域制御可能なインターネット部、各種の FireWall や IDS を備え、DNS/SMTP/Web などのサーバを擁する被害者部からなる(図 1)。

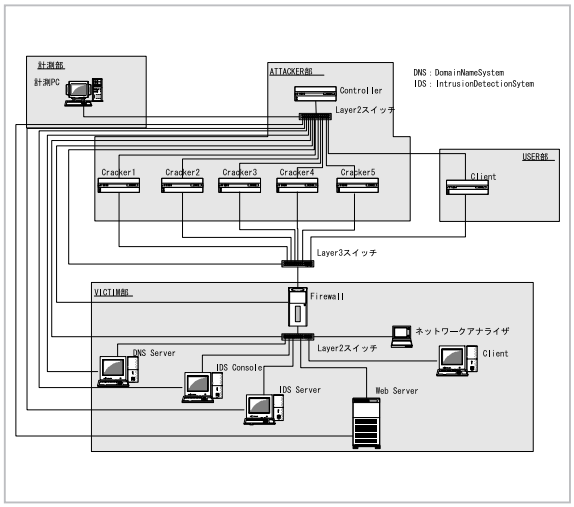

図1 SIOS 不正アクセス再現実験装置

さらに、現在は構成を柔軟化し、攻撃再現部の 100 ノードは攻撃再現部としてだけでなく、被害者部やインターネット部として、それぞれ個別に役割を割り当てることが可能となっている。

実際の攻撃ツールを利用して、最大 100 ノードからの DDoS 攻撃を模倣でき、実際の実装を用いて被害者への影響を模倣できる。

また、実験の管理や計測を行うためのエージェントが実装され、実験の遂行の自動化が図られており、実機による大規模な実験環境でありながら、詳細な実験管理を可能とし、運用の負担を軽減している。

1　SIOS は Security Inteligent Operation Studio の略で、独立行政法人 通信総合研究所（現情報通信研究機構）非常時通信グループが横河電機株式会社と共同で開発したシステムである。このシステムを元に横河電機株式会社が独自に商品化したものが、商品としての SIOS であり、同社の登録商標となっている。

2.2　VM Nebula

VM Nebula[2] は、PC エミュレータによる実験環境である。実機による実験環境の再現精度とエミュレータによる実験環境の柔軟性、耐規模性を兼ね備えることを一つの目標とした環境である。兵庫県神戸市にある情報通信研究機構の関西先端研究センターに設置されている。

VM Nebula は、PC エミュレータが動作する 4 台の模倣サーバとそれらを物理接続する 2 台のマルチレイヤスイッチからなる（図 2）。

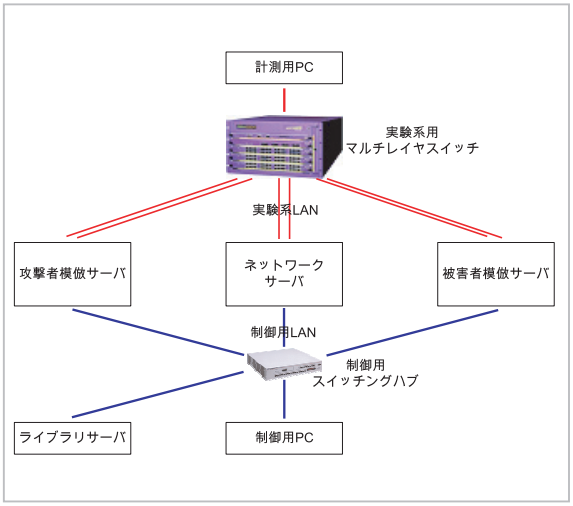

図2　VM Nebula

サーバはすべて等価であり、2 台のマルチレイヤスイッチはそれぞれすべてのサーバへと接続しているため、各サーバには機能上の違いはない。そのため、それぞれの役割は変更可能であり、かつ、それぞれの役割への機器の割当ても任意である。

攻撃者や被害者の PC は、PC エミュレータを用いた仮想 PC によって模倣される。FireWall や IDS、各種のサーバからなる被害サイトは、複数台の仮想 PC によって模倣される。インターネットは、マルチレイヤスイッチを介して VLAN による接続と帯域制限を行うとともに、ルーティングソフトウェアを実行する仮想 PC を仮想ルータとして用いることで模倣する。

実際の OS 実装やサーバ実装をそのまま用いることができ、攻撃ツールなども PC 上で動作するものをそのまま利用することができる。

仮想 PC の構成やマルチレイヤスイッチの設定などを保存、配布する機能を持っているため、一度構成した実験系を再度構成することや再利用することが容易にできる特徴があり、頻繁に再実験を必要とするウィルスやワームの解析[3] などにも用いることができる。ただし、実験の遂行を自動化する仕組みは現在のところ提供されていない。

2.3　StarBED

StarBED[4] は石川県能美市にある情報通信研究機構の北陸 IT 研究開発支援センターの愛称で、大規模なネットワーク実験を行うための施設である。

StarBED は 512 台の PC とこれらを接続するスイッチ群で構成されている。それぞれの PC には 2 個以上のネットワークインターフェースが用意されており、実験用ネットワークと管理用ネットワークへそれぞれ接続されている。これは、実験用トラフィックと管理用トラフィックを分離するために必要な機能であり、これにより想定外のトラフィックによる実験結果への影響を防ぐことができる。管理側のネットワークには実験を支援するためのファイルサーバや DHCP サーバ、また我々が開発している実験環境の自動構築及びシナリオの自動遂行を実現するためのアプリケーションが動作するノードが設置されている（図 3）。

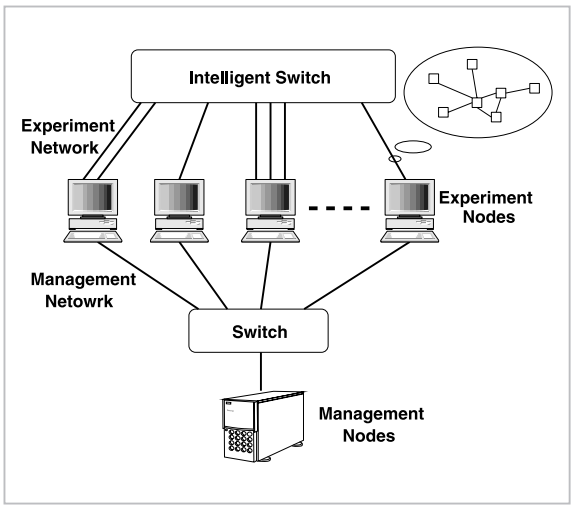

図3　StarBED

基本的に各ノードやスイッチの物理的トポロジを変更せず、スイッチ群の設定を変更することで実験用トポロジを構築する。これにより、複数の利用者による同時利用や、実験用トポロジの構築のコストを軽減している。利用者は、各ノードのシミュレーション用のネットワークインタフェイスが収容されているスイッチの設定を変更することで、必要な実験トポロジを構築する。

実験支援ツールを利用することで、利用者は実験の設定記述を行うだけで、実験トポロジの構築及び実験の遂行までが自動的に行われる。

3 統合実験

今回の実験は、統合の予備実験として、主に接続環境の性能に関して実験を行った。本節では、その実験について述べる。

3.1 接続環境

三つの実験環境の物理接続には、JGNⅡを用いた。これは、主に以下の3点の理由による。

- 広帯域な(10Gbps)ネットワーク接続を用意できること。
- 実験専用線でインターネットとは別の隔離されたネットワークであること。
- 三つの実験環境がいずれもJGNⅡのアクセスポイントに近く、低いコストで接続環境を準備できること。

接続に際しては、JGNⅡの「多地点同時接続サービス」によるEthernet接続で三つの地点を結び、複数のVLANを必要に応じて張り替えながら[2]利用する。東京都小金井市と石川県能美市の間は10Gbpsで、兵庫県神戸市との間は1Gbpsで接続される。

各VLANの用途としては、以下を想定しており、余剰1本を含め、標準状態で4本のVLANを用意している。

- 実験環境の運用、制御、計測情報用
- 相互の遠隔操作用
- 実験上のノード間の通信用

ルーティングを行わないレイヤ2の接続で、運用管理に利用するIPアドレスなどは調整する必要がある。

2 本来このような方式はサービスされておらず、今回特別にサービスして頂けることとなった。VLANの張り替えは手動で行う。

3.2 接続実験

接続実験では、VM NebulaとStarBEDを「実験環境の運用、制御、計測情報用」のVLANを用いて接続した。接続図を図4に示す。

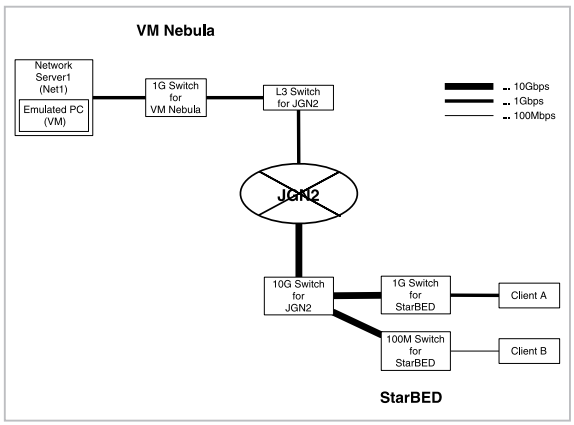

図4 VM NebulaとStarBEDの接続図

実験に利用したノードのNICとOSを表1に示す。

実験に利用したすべてのノードには、同じネットワークに属するプライベートIPアドレスを付与した。

接続性能を測るために、今回は`ping`コマンドによるRTTの計測と、`netperf`[5]を用いた`TCP_STREAM`と`UDP_STREAM`の性能について測定した。結果を表2に示す。なお、`TCP_STREAM`と`UDP_STREAM`はスループットで単位はMbps(10^6bits/sec)、RTTは`ping`コマンドで100回`ICMP`を送信したときの平均RTTで単位はmsである。

表を見る限り、VM NebulaとStarBED間の`TCP_STREAM`のスループットが最大約12分の1と異常に低い。特に、それぞれの実験環境内では、`TCP_STREAM`は`UDP_STREAM`と同程度かそれ以上であることから、JGNⅡを介した接続でのみ何らかの異常が発生している可能性がある。これに関しては、調査したところ、LFN問題[3]であることが判明した。

`UDP_STREAM`に着目してみた場合、Gigabit Ethernetのインターフェースで接続している

表1　実験ノードのNICとOS

環境	ノード	略称	NIC	OS
VM Nebula	ネットワークサーバ1	Net1	1000Base-SX	RedHat Enterprise Linux AS 3.0
	仮想PCノード	VM	1000Base-SX	FreeBSD 5.3R
StarBED	Client A	A	1000Base-T	FreeBSD 5.3R
	Client B	B	100Base-TX	FreeBSD 4.4R

表2　実験結果

Sender	Receiver	TCP_STREAM	UDP_STREAM	RTT
VM Nebula intra				
Net1	VM	159.90	137.39	0.252
VM	Net1	298.90	152.30	0.252
VM Nebula→StarBED				
Net1	A	45.14	549.36	8.711
Net1	B	15.32	95.78	8.668
VM	A	28.40	152.63	10.580
VM	B	15.08	95.54	11.007
StarBED→VM Nebula				
A	Net1	24.25	412.70	8.754
A	VM	20.10	117.98	8.925
B	Net1	14.38	95.75	8.766
B	VM	14.28	93.24	8.747
StarBED intra				
A	B	93.24	95.88	0.228
B	A	93.38	95.93	0.211

Net1とAの間で約400〜550Mbps程度のスループットである。これは、各ノードの処理性能やJGNⅡを介した場合の限界性能であると考えられる。また、100Base-TXのインターフェースで接続しているBでは、どのノードとの間でも約90〜95Mbps程度のスループットが限界となっており、これはネットワークインターフェースによる限界と考えられる。

これに対し、VMとAとの間では、約100〜150Mbps程度のスループットがある。これは、VM Nebulaの内部での性能と同程度であり、仮想PCソフトウェアやその実行サーバの性能による限界と考えられる。

3　Long Fat Network問題のこと。回線の帯域遅延積（キャパシティ）よりTCPのWindow Sizeが小さい場合に、転送性能がWindow SizeとRTTで制限されてしまう現象のこと。近年のTCP実装ではWindow Size Scaleオプションを利用することで、この問題を回避できるようになっている。今回用いたOSでも同オプションが実装されていたが、なぜか機能していないことが判明した。なぜ機能しなかったのかは、調査中である。

3.4　大規模攻撃模倣実験

次に、JGNⅡで接続されたSIOSとVM Nebula、StarBEDの三つの再現実験環境を用いて、大規模な攻撃を模倣する実験を行った。

内容は、下記のような単純なものである。

(1) F5攻撃によって対象Webサーバがサービス不能に陥る。
(2) 移動型フィルタの適用により対象Webサーバがサービス可能に復帰する。

F5攻撃は、最近サイバーデモンストレーションなどによく利用される攻撃手法で、電子掲示板などで申し合わせた時刻に、特定のWebページを表示したInternet ExplorerのFunctionキーF5を押すというもの。F5キーは“Reload this page”に割り当てられており、多くの人が同時に押すことで、大量の`HTTP request`が対象となるWebページを提供しているサーバに送られる。これによるrequestでサーバへの下り帯域があふれたり、許容request数を超えたり、当該requestに対するresponseでサーバからの上り回線帯域があふれたりするなどのフラッディングを目的とした攻撃である。原始的なDDoS攻撃でIPアドレスなどは詐称しない。

移動型フィルタとは、フィルタの適用点を移動させる技術の総称である。帯域浪費型のDDoS攻撃などでは、組織の出入口にあるFireWallでパ

ケットを廃棄したとしても、組織の出入口の帯域が不足している場合には、意味をなさない。そのため、一般的に上流にあたるプロバイダーなどの外部組織に依頼して、関連するパケットをより発信元に近いところでフィルタしてもらう。現在手動で行われているこのようなフィルタをIPトレースバック技術などと組み合わせ、自動的に攻撃の発信元近くまでフィルタの適用点を移動する技術を移動型フィルタという。現在幾つかの方式が提案されているが、いずれもまだ実現段階にない。なお、今回の実験では、シナリオ記述に従って順次フィルタが起動するだけで自動的にフィルタが移動する移動型フィルタを実装しているわけではない。

実験の構成は、「SIOSから攻撃し、StarBED上のルータを経由して、VM Nebula上のサーバに被害を及ぼす」こととし、詳細は下記のとおりである(図5参照)。

- SIOSのAttackerノードを10台程度用いてHTTPのrequestを繰り返す(F5攻撃の模倣)。
- すべての攻撃が別経路で到達するようにStarBEDでは50台程度のルータを用意(現実的なインターネット上の遅延等の模倣)。
- VM Nebula上にはFireWallとWebサーバをそれぞれ別の仮想PCとして構築(対象サイトの模倣)。

SIOSのAttackerノードでは、`HTTP request`トランザクションを繰り返すスクリプトを自動実験遂行機能で実行することで攻撃を模倣する。Attackerノードは15台とし、15台が一斉にトランザクションを実施するよう構成した。

StarBED上には、ルータとしてルーティングソフトウェア`zebra`を用いたPCルータを54台構築し、経路は、経路の異なる複数のサイトからの攻撃を模倣するため、ノードごとに経由ホップ数を違えるように構成した。また、一部のPCルータにはFireWallソフトウェア`ipfw`を起動することによって移動型フィルタを実現するスクリプトを導入した。

VM Nebula上には仮想PC上でFireWallソフトウェア`ipfw`を動作させたFireWallとWebサーバソフトウェア`apache`を動作させたWebサーバを構築した。

攻撃が開始されると、SIOSの自動実験遂行機能を利用して、15台のAttackerから同時に`HTTP request`のトランザクションが繰り返し発生される。Attackerノードから発せられた`HTTP request`は、StarBED上のPCルータを経由してVM Nebula上のFireWallを越え、VM Nebula上のWebサーバに到達する。

攻撃開始直後から対象Webサーバにアクセスができない状態になることが確認された。その後、移動型フィルタを起動すると、Webサーバへのアクセスが可能な状態に復帰することも確認された。

なお、AttackerノードからWebサーバまでのRTTは25ms～400msと大きなばらつきがあり、Webサーバへのアクセスが可能なはずの攻撃開始前やフィルタ起動後でもアクセスが不安定な状態も散見されたことも記しておく。

4 考察

前節の実験結果を踏まえて、実験環境の連携における接続について考察を加えることとする。

実験環境を連携させる上では、様々な情報を流通させる必要がある。その中でも、インターネットセキュリティ事案の再現に最も重要なのは、事案の各要素(攻撃ホスト、仲介ホスト、被害ホストなど)を模倣する実験ノード同士の通信であると考えられる。なぜなら、インターネット上のセキュリティ事案は何らかの通信によって発生するため、その再現は、どんな通信によってどんな事象が引き起こされるのかを模倣することで行うからである。

複数の実験環境にまたがって実験ノード同士が通信する場合には、通信帯域や実際の性能(スループットやRTTなど)が再現する通信に適しているかを把握しておく必要がある。

VM Nebulaでは、実際に実験ノードとして用いるのはすべて仮想PCノードである。よって、VM NebulaとSIOSやStarBEDを連携させる場合には、VM Nebulaの仮想PCノードとSIOSやStarBEDの各実験ノードを接続し、実験することとなる。そのため、留意すべきは、仮想PCノードとSIOSやStarBEDの各実験ノード間の性能である。

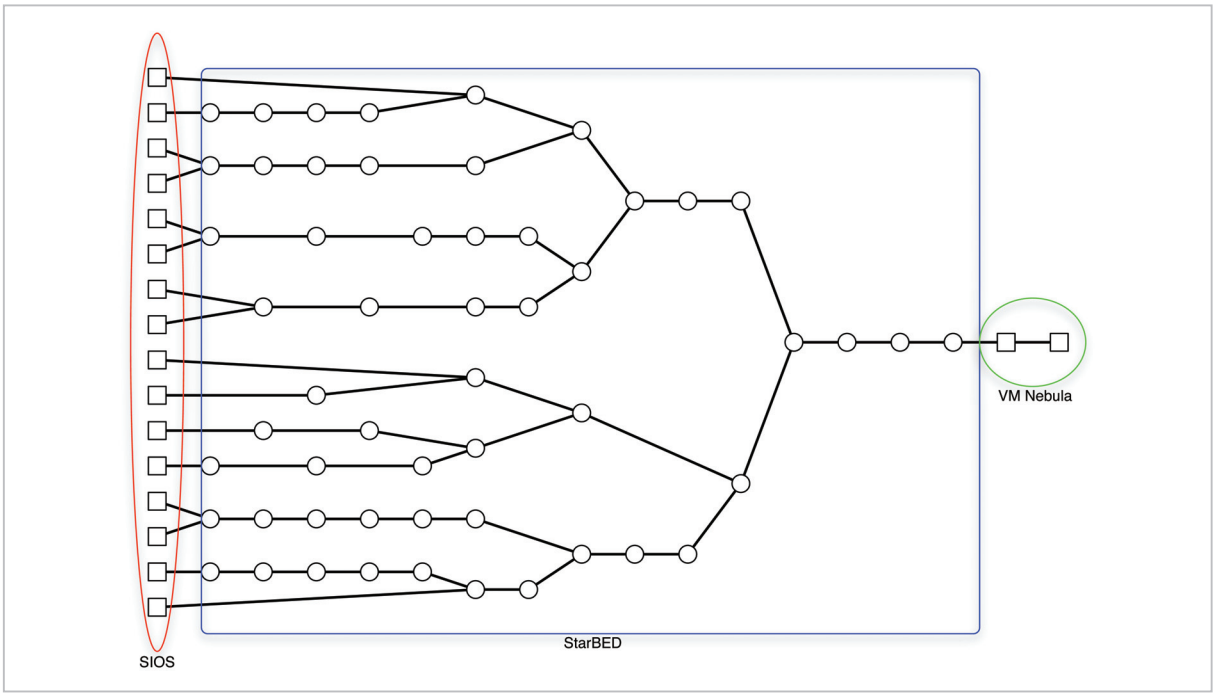

図5　模倣実験の構成図

表を見る限り、UDP_STREAM のスループットは、仮想 PC ノードと StarBED の各ノード間では、VM Nebula 内部の性能と同程度か、StarBED 側ノードのネットワークインターフェースの性能を限界としている。StarBED 側ノードはネットワークインターフェースよって Class 分けされており、実験に必要なネットワークインターフェースを持ったノードを選択できる。よって、VM Nebula 内部の仮想 PC ノードの性能が、StarBED と連携した場合の接続性能の上限であることを踏まえて、各種の実験を構成する必要がある。

実際には、複数の仮想 PC ノードを動かした場合には、今回の実験より更にスループットが低下することが予想されるため、SIOS や StarBED との間で再現する要素の割当などを十分に検討して配分することが求められる。

また、RTT を見ると VM Nebula 内なら 1ms 以下であるが、StarBED との間では約 8〜11ms 程度ある。これは、SIOS との間でも同様で、さらに、VM Nebula から StarBED 上の PC ルータ 1 台を経由して SIOS に到達するような場合には、約 25ms〜40ms と変動がある。

このように、通信性能に関して詳細な結果を得るには、複数環境をまたぐ実験の場合、留意する必要があると考えられる。

6　おわりに

本稿では、不正アクセス等の再現実験環境の統合手法を検討するに当たって、我々が研究開発してきた VM Nebula と StarBED を用いて行った接続実験と、SIOS と StarBED、VM Nebula を用いた模倣実験について述べ、考察を加えた。100Mbps 程度のホスト間の通信の再現であれば、特に大きな問題を生じることなく大規模な再現実験が可能と考えられる。

今後は、更に大規模な事案再現を試みるなど、統合による効果を検証していく予定である。

謝辞

本研究の研究費用は、科学技術振興機構の科学技術振興調整費によって賄われている。有用な研究費を与えて頂いた関係各位には、記して感謝の意を表したい。

参考文献

1 大野　浩之，武智　洋，永島　秀己，“インターネットの脅威に対抗しうる脆弱性データベースと検証システムの構築”，情報処理学会，分散システム／インターネット運用技術（DSM）シンポジウム 2001，Feb．2001.

2 三輪　信介，滝澤　修，大野　浩之，“仮想 PC インターネットセキュリティ実験環境『VM Nebula』の設計と構築”，電子情報通信学会，2003 年　暗号と情報セキュリティシンポジウム（SCIS2003），Jan．2003.

3 三輪　信介，大野　浩之，“再現実験環境『VM Nebula』を用いたウィルス・ワームの解析”，Internet Conference　2003，Oct．2003.

4 Toshiyuki Miyachi, Ken-ichi Chinen, and Yoichi Shinoda, "Automatic Configuration and Execution of Internet Experiments on an Actual Node-based Testbed", Tridentcom2005, Trento, Italy, ISBN 0-7695-2219-X, pp.274-282, Feb, 2005.

5 The Public Netperf Homepage, <URL: http://www.netperf.org/netperf/NetperfPage.html>.

三輪信介（みわしんすけ）
情報通信部門セキュアネットワークグループ研究員　博士（情報科学）
ネットワークセキュリティ

大野浩之（おおのひろゆき）
情報通信部門セキュアネットワークグループリーダー　理学博士
コンピュータネットワーク、危機管理