不正アクセス等再現・模倣実験環境の統合手法に関する考察

三輪 信介* 大野 浩之*

インターネット上では時々刻々と新たな攻撃手法が考案され，実行されているため，それらを再現・模倣し，その影響や対策の有効性を検証できる実験環境の構築は重要である．

しかし，攻撃事案は，年々大規模かつ複雑化し，単一の実験環境での再現・検証は困難になって来ている．

そこで，本稿では，我々が研究開発してきた複数の不正アクセス等の再現・模倣実験環境を挙げ，これらの相互接続手法や統合運用・管理手法についての議論を通じて，不正アクセス等再現・模倣実験環境の統合のあり方について述べる．

A study of an integration method of simulating environments for the Internet security incidents

Shinsuke Miwa† Hiroyuki Ohno†

In the recent trend of attacks on the Internet, an attack either trades on some imperfect mechanism of the Internet, or perverts extensive hosts or sites that have deficient security against attacks. The attack sometimes defeats hosts or sites that have sufficient security against attacks, and sometimes has a considerable effect on the Internet widely.

To against these attacks, new countermeasure technologies must be puzzled out from deal with the whole components of the Internet.

Considerable number of experiment environments to simulate these attacks and their efficients were researched and developed. However, we have difficulties to simulate recent security incidents because they extend their scale and complexity.

In this paper, we deal with an integration of simulating environments for the Internet security incidents through some experiments to integrate between simulating environments.

1 はじめに

インターネット上での種々の攻撃手法に対し，その影響や対策の有効性を検証する実験環境の構築には，さまざまな手法が用いられており，何をもって正しい検証とするかを見極めることは困難である．

そこで，本稿では，いくつかの実験環境を統合する試みを行い，それを通じて，不正アクセス等の再現・模倣実験環境にとって不可欠な要素やその能力の基準となるものを導き出すことを目指す．

本稿で述べる実験環境とは，コンピューターネットワーク，特にインターネットにおける不正アクセス等の再現実験環境を意味し，各要素間での通信や各要素の挙動を再現・模倣し，それらを計測することで，攻撃の影響や対策の効果などさまざまな結果を得ることを目的としたものである．

また，本稿における統合とは，複数の実験環境が相互に影響し合い，かつ，統一的に管理・運用することが可能な状態を指す．

*独立行政法人 情報通信研究機構 情報通信部門 セキュアネットワークグループ

†Secure Networks Group, Information and Network Systems Division, National Institute of Information and Communications Technology

2 相互接続

複数の実験環境を統合するためには，互いに影響を与えられるようにする何らかの接続が必要である．本章では，実験環境の相互接続について述べる．

本稿においては，実験環境内の対象要素（以降ノードと呼ぶ）について，ノード自身の状態変化などの内部挙動と通信による外部への影響を実験の対象とし，その他の挙動や影響は対象外として，再現・模倣や計測を必要としない．

そのため，相互接続においては，実験環境間でノード同士の通信による影響をどのように伝播するかが重要である．

2.1 物理的接続

まず，相互接続としてそれぞれの実験環境間で通信を行えるようにする物理的接続が考えられる．物理的接続を果たせば，相互接続が実現されるように感じられるが，実際にはそうではない．

例えば，NS[1] などのシミュレータを実行している計算機と実機による実験環境を物理的に接続したとしても，実験環境同士が相互に影響を及ぼすことができるわけではないからである．

逆に，物理的に接続を果たしていなくとも，相互に影響を与えることは可能である．例えば，シミュレータに他の実験環境で得られた挙動を入力すれば，シミュレータ内部の挙動に影響を与えることが可能だからである．

このように，物理的接続は実験環境の相互接続に対する十分な条件でも必須の条件でもない．

2.2 論理的接続

次に，相互接続としてそれぞれの実験環境で何らかの影響を伝達する論理的接続が考えられる．シミュレータへ他の実験環境で得られた挙動を入力するなどがこれにあたる．

通信を物理的な通信で実現する実機による実験環境やハイブリッド環境（の一部）では，論理的接続は物理的接続の上に成り立っている．よって，このような環境の論理的接続には，物理的な接続が不可欠である．

シミュレータでは，論理的接続はシミュレータソフトウェア同士の接続やプロセス間通信など必ずしも物理的接続を必要としない．

問題は，シミュレータと実機による実験環境を接続するような場合である．シミュレータは，ある種のソフトウェアであり，シミュレータ内のノードの挙動はすべて，そのソフトウェアの実行実体（プロセスなど）に閉じている．

よって，外部に接続するためには，シミュレータから実ネットワークなどへの変換が必要になる．そのための手法として，NSE[2, 3] や N*(NStar)[5] がある．

2.3 遠距離接続

地理的に離れたところにある実験環境同士を物理的に接続する必要がある場合には，いくつかの問題がある．

物理的な回線を確保することが困難であるということが一つである．近年では，安価に高速な回線を用意することができるようになってきたが，それでも長距離の専用回線を用意するのは困難である．

RON[4] などを用いて，インターネットを利用する方法も考えられるが，セキュリティや実験とは無関係の第三者に影響を与えないなど独自の配慮が必要となる．

また，回線が確保されたとしても，その帯域や遅延によって実験環境をまたがる通信は影響を受けることになる．特に，インターネットを介する場合には，経路制御や回線状況による影響があるため，より複雑になると考えられる．

回線状況に関する問題を解決するための消極的な解決方法としては，実験環境をまたぐ通信が回線状況などの影響などを許容できるようなものに限定されるような実験系の設計を行うことが考えられる．

積極的な方法としては，中間に何らかの変換要素を用意し，回線状況による影響をその要素で吸収することが考えられる．

3 相互運用

複数の実験環境を統合するためには，双方を一つの運用主体によって管理，運用できる必要がある．本章では，実験環境の相互運用について述べる．

相互運用においては，それぞれの管理・運用をどのように行うか，相互の管理における違いをどのように吸収するかが重要である．

3.1 遠隔操作

まず，複数の実験環境がある場合には，それぞれを操作できる必要がある．物理的に一つの計算機の中で実現されている場合には，なんら特別なものを必要としないが，多くの場合は，実験環境は物理的にも分離している．そのため，操作にはなんらかの遠隔操作が必要となる．

BSD系やPOSIX準拠のUNIXシステムであれば，リモートShellやそれに類するもので操作ができるだろうし，X window systemも遠隔操作を提供している．その他のOSでも，多くが何らかの遠隔操作手段を提供している．また，VNC[6]は多くのOSで，インターネットを経由した遠隔操作を可能とする．

また，KVMスイッチや遠隔KVMなどを用いることも遠隔操作の選択肢となりうる．[7]

3.2 さまざまな違い

このような遠隔操作環境を用いることで，運用上の操作に関しては，相互に行うことが可能となるが，それだけで相互運用を果たしたとは言えない．

どの程度忠実に再現するかといった再現の正確性や，時間の取り扱い方，何を計測できるかといった計測の能力，制御がどの程度細かくできるのかといった粒度などは，実験環境毎に固有である．

相互運用を行うには，これらの違いを十分に考慮した上でそれぞれの実験環境の利用方法を決定し，場合によっては，これらの違いを吸収する機構を導入するなどが必要となる．

4 手法の検討

第1章に示したとおり，本稿において，統合を果たしたと言えるのは，実験環境が相互に影響し合い，かつ，統一的に管理・運用することが可能な状態である．

本章では，統合する上で，いくつかの手法を検討し，その特徴などについて考えてみる．

4.1 相互接続と遠隔操作

論理的な接続を含めた相互接続を行い，相互に遠隔操作を可能とすることで，統合を果たしたということができる．

ただし，この場合には，3.2節に述べたような違いを吸収できないため，それぞれの実験環境の特性に応じて，どの実験環境にどのノードを配するかなどに十分な注意を行う必要がある．

4.2 変換機構の導入

論理的な接続を含めた相互接続を行い，3.2節に述べたような違いを吸収するための変換機構を導入した場合，統合を果たしたということができる．

この場合には，変換機構によって違いを吸収するために，実験環境間の違いは意識する必要が無い．しかし，その代わり，それぞれ実験環境の持つ優位性を変換によって失ったり，全体としての能力が低下するなどの可能性がある．

4.3 併合

論理的な接続を含めた相互接続を行い，一つの実験環境の管理方式で全体を管理するように変更した場合，一つの実験環境に併合する形で統合を果たしたと考えることができる．

ハイブリッド環境は，このような形での統合の例である．Emulabでは，実際にNSE環境が実機による実験環境内に併合されている．

併合の場合には，設計段階で十分に考慮されていなければ，実験環境に大幅な変更が必要となると考えられる．

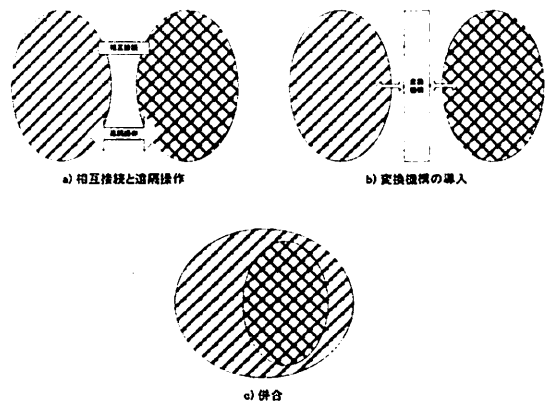

図 1: 統合手法

5 統合実験

実験環境の統合のあり方を探るために，複数の実験環境の相互接続や相互運用の実験を行い，手法を検討する必要がある．本章では，我々が研究してきた2つの実験環境について，各環境を概説し，その上で，遠距離にある2つの実験環境間での遠隔操作と相互接続による統合実験について述べる．

5.1 各実験環境の概説

統合実験で用いる2つの実験環境それぞれについて，概説する．

5.1.1 不正アクセス再現実験装置

大野らによる不正アクセス再現実験装置[8]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．

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2)

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．

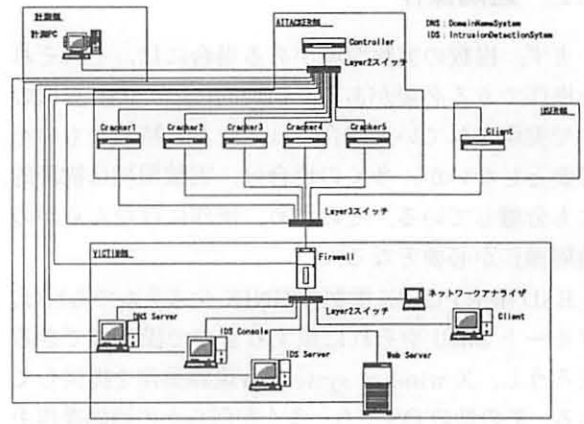

図 2: 不正アクセス再現実験装置 (SIOS)

5.1.2 VM Nebula

VM Nebula[9]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．

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3)

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無い．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り当ても任意である．

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る．

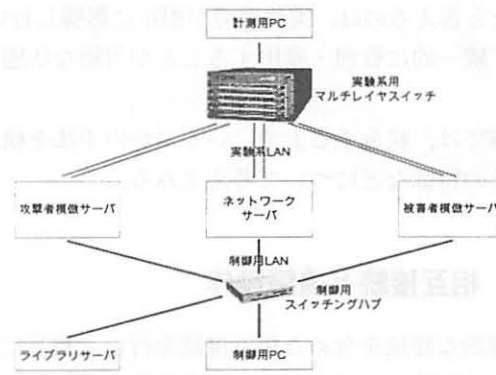

図 3: VM Nebula

[1] Security Intelligent Operation Studio

5.2 実験における留意点

統合実験を行う上で，留意すべき点について述べる．

5.2.1 同期性

今回用いる，不正アクセス制限実験装置は，実機による実験環境であり，VM Nebula はエミュレータによる実験環境である．

このような，違った種類の実験環境を統合する場合には，同期性に留意する必要がある．

まず，それぞれの実験環境でのイベント発生順序が正しく同期されねばならない．環境に差がある際には，多くの場合，時間の進み方やイベント生起のタイミングなどにずれがあるため，正しく再現することができなくなる．

また，それぞれの実験環境間で，時刻の同期を取る必要がある．同期がとれていない場合には，それぞれの実験環境で記録されるログなどの時刻記録にずれが生じ，正しい記録として用いることができないからである．

5.2.2 隔離性

今回用いる 2 つの実験環境は，それぞれ遠隔地に存在している．不正アクセス再現実験装置は，東京都小金井市にあり，VM Nebula は兵庫県神戸市にある．

これらの間は，拠点間を結ぶ 100Mbps の広域 Ethernet によって LAN 接続されているが，専用の回線ではなく，拠点間の事務や他の研究上のやり取りも同じ回線を利用して行われる共用回線となっている．この他に，各実験環境には専用の最大 6Mbps 程度の ADSL 回線が用意されている．

このような共用回線やインターネットを介して，遠隔操作や相互接続を試みる場合には，実験環境の隔離性に留意する必要がある．

まず，本来の操作権限を持つ者以外による不正な遠隔操作や覗き見などを排除しなければならない．実験内容の漏洩や実験結果への悪影響が考えられるからである．

また，外部からの実験環境への攻撃などを含む不必要な通信は，抑制もしくは排除せねばならない．本来の再現しようとしている攻撃による影響と外部からの通信の影響が分離されていなければ，正確な再現ができないからである．

同時に，扱う内容がセキュリティであるがゆえに，実験環境の内側から共用回線やインターネットを介して，外部に悪影響を与えないように配慮する必要がある．例えば，ウィルスやワームなどが相互接続回線から共用回線などを通して，外部に流出感染してしまうことは，避けねばならない．

さらに，実験に伴って，帯域が大量消費されるなどの過度な通信負荷が発生することで，二次的影響が外部に及ぶことも抑制せねばならない．

5.3 実験

本稿では，統合実験における統合の手法として，最も単純な，4.1 切に述べた「相互接続と遠隔操作」を用いて，統合を試みることとする．

5.3.1 遠隔操作

遠隔操作は，Internet Protocol を使ってキーボードやマウスの操作イベントと画面を伝送できる KVM over IP 装置 [10] を用いて，ADSL 回線を介して行うこととした．接続関係を図 4 に示す．

ADSL 回線を利用したのは，

- KVM over IP を利用する上では ADSL 回線程度の帯域で十分と考えた
- インターネットを介して外部からも利用可能としたい

などの理由による．

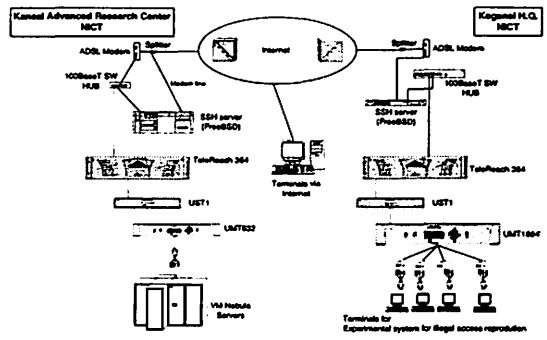

図 4: KVM over IP による遠隔操作

外部からの不正な操作を防止するために，KVM over IP 装置には認証機能が用意されているが，KVM over IP 装置と操作者との間の通信は保護されない

ため，覗き見や改ざんによる操作の妨害を防ぐことはできない．

そこで，実験では，SSH のポートフォワード機能を利用することとし，ADSL 回線に接続された SSH サーバを介して，KVM over IP 装置と通信することとした．

5.3.2 相互接続

相互接続は，物理接続には共用回線である 100Mbps の広域 Ethernet を利用し，論理接続は実験環境間で VPN を構築することとした．

共用回線を利用したのは，

- 拠点間の通信以外がないためある程度の隔離性が期待できる
- 大量の通信を利用するような攻撃の再現には太い帯域が必要と考えられた

などの理由による．

不正アクセス再現実験環境と VM Nebula の両方ともに，制御系はプライベートアドレス空間に接続されている．再現を行う駆動部では，一般にはプライベートアドレス空間を用いているが，再現における需要があればグローバルアドレス空間を用いることも可能となっている．よって，全てのアドレス空間を VPN を使って，接続する必要がある．

実験では，IPsec トンネリングによる IPsec VPN を構築し，実験内容の漏洩や外部からの妨害通信の排除にも配慮した．

さらに，外部からの不必要な通信の流入と外部への攻撃などの流出を避けるために，両方の実験環境の出入口に FireWall を設置して，IPsec トンネルを介した通信以外が出入りしないようにした．

また，実験による帯域の極端な減少などの二次的影響を避けるために，`dummynet` を利用して帯域制限を行うこととした．

6 実験結果と考察

遠隔操作に関しては，前述のような環境を使って，相互に操作をすることができることを確認した．ただし，ADSL 回線や KVM over IP 装置の問題から，GUI を使った操作は不自由であり，何らかの対策が必要であると思われた．

今回用いた 2 つの実験環境は，いずれも実時間ベースで動作し，実際に通信パケットをやり取りし，実際の OS 実装やサーバソフトウェア実装を動作させる．そのため，同期性に関しては，`ntp` による時刻同期程度で，それ以外に特に対策は行っていない．実際には，VM Nebula では PC エミュレータの問題から，時間の進み具合が若干実時間とは異なっているため，何らかの対策が必要であると考えている．

相互接続に関しては，現在，準備中であり，近いうちに報じることができる予定である．

7 おわりに

本稿では，インターネットにおける不正アクセス等の再現・模倣実験環境について，そのあり方を，我々が研究してきた実験環境の統合実験を通じて述べた．

参考文献

[1] VINT Project, ⟨URL: `http://www.isi.edu/-nsnam/vint/index.html`⟩.

[2] K. Fall, "Network Emulation in the Vint/NS Simulator", *In proceedings of the 4th IEEE Symposium on Computers and Communications*, 1999.

[3] VINT Project, "Network Emulation with the NS Simulator", ⟨URL: `http://www.isi.edu/nsnam-/ns/ns-emulation.html`⟩.

[4] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris, "Resilient Overlay Networks", *In Proceedings of 18th Symposium on Operating Systems Principles (SOSP)*, ACM, pages 131–145, Oct. 2001.

[5] 宮地 利幸, 宇夫 陽次郎, 森島 直人, 篠田陽一, "N*(NStar): ns-2 の real external interface の構想", 情報処理学会, マルチメディア通信と分散処理, 103-20, 2001.

[6] Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood, Andy Hopper, "Virtual Network Computing", IEEE Internet Computing, pp33-38, Vol.2 No.1, Jan/Feb 1998.

[7] 大野 浩之, 松本 文子, 山崎 靖博, "高度情報通信危機管理研究施設の構築", 情報処理学会, 分散システム／インターネット運用技術研究会, Apr. 2003.

[8] 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, DSM シンポジウム 2001, Feb. 2001.

[9] 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), 2003.

[10] 大野 浩之, 山崎 靖博, 松本 文子, 三輪 信介, "高度情報通信危機管理研究施設の構築 – (2) 研究施設間接続方式の設計と実装", 情報処理学会, 分散システム／インターネット運用技術研究会, Sep. 2003.