2-3　不正アクセス再現実験環境 SIOS、VM Nebula の構築とその応用

2-3 A Development of Experimental Environments "SIOS" and "VM Nebula" for Reproducing Internet Security Incidents

三輪信介　大野浩之
MIWA Shinsuke and OHNO Hiroyuki

要旨

インターネット全体の要素を考慮して根本的な解決を図るような新たなセキュリティ対策技術が求められているが、インターネット上で起こる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、原因の究明や対策の立案は、より困難になってきている。

このような状況に対し、我々は対策技術の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。本稿では、不正アクセス再現実験環境について、その意義と目的を概観した上で、我々が研究開発してきた SIOS 及び VM Nebula について概説し、今後の展望を含めて述べる。

Security incidents are growing significantly on a daily basis in the Internet world causing considerable damage. To protect against these incidents, some protection mechanisms or softwares has come to be used. Each time a new attacking method or virus or worm appears, it must be analyzed in detail since such protection mechanism or software requires detailed information on that. However, these incidents are sophisticated because enlarged its scale and supervened incidents cause many interactions, make it difficult to acquire such in-depth information.

To analyze sophisticated incidents, we developed experimental environments for reproducing Internet security incidents. In this paper, we report on the development of our reproducing environments called "SIOS" and "VM Nebula".

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

1　はじめに

近年の情報通信システムは、コンピュータシステムとそれらを結ぶネットワークを中心として発展してきた。特に、インターネットの普及に伴い、多くの一般市民、民間企業のみならず、政府機関のコンピュータシステムまでもが、インターネットを介して接続されている。

インターネットは世界規模のコンピュータネットワークであり、企業にとっては、営業活動の展開や電子商取引の基盤となっている。個人にとっては、情報交換の基盤環境であり、情報収集のための重要なツールともなっている。また、多くの組織は、インターネットを情報発信に利用している。さらに、電子政府を実現するに当たっては、インターネットは欠かせない重要インフラとなるだろう。

このインターネットの急速な普及と利用の拡大と同時に、情報通信システムは、データの破壊や改ざん、システムそのものの破壊やサービスの不能化、個人情報や企業機密の漏えいなど、多くの脅威にさらされるようになってきている。

さらに最近では、広帯域常時接続環境の普及や、攻撃手法の高度化に伴い、一般に広く脅威が蔓延している状況にある。

インターネットが重要な社会インフラとして、その機能を適確に果たし続けるためには、脅威を排除し、安心して使える安全で快適なものでなければならない。

しかし、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といえるだろう。

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[1][2]してきた。

そこで、本稿では、不正アクセス再現実験環境の意義と目的を概観した上で、我々が研究開発してきたSIOS[1]及びVM Nebulaについて述べ、さらに複数の実験環境を連携させて大規模かつ複雑な事案を再現する試みについて述べる。

1 SIOSはSecurity Intelligent 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。このシステムを基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 情報通信システムセキュリティ研究の概要

我々の行ってきた研究開発の位置付けを明らかにするために、情報通信システムに対してどのような脅威があるのか、それに対してどのような対策が、どのような技術を用いてとられるのかを、インターネットセキュリティを中心に述べる。

2.1 情報通信システムに対する脅威

インターネットを介して接続されている情報通信システムでは、情報はオープンなネットワークを介して伝達されるため、システムやその利用者は常にセキュリティ上の脅威にさらされている。

その脅威を大まかに分類すると、盗聴、改ざん、なりすまし、不正アクセス、サービス妨害が挙げられる。

これらの脅威の多くはインターネットを介してもたらされるが、物理的な機器の持ち込みによるウィルス・ワームの感染や、電磁波を利用した盗聴やサービス妨害などのように、インターネット以外の媒体を介してもたらされる脅威も存在している。

盗聴・改ざん・なりすましに対しては、現在のインターネットがこれらを防ぐための機能を提供していないために、利用者が何らかの対策を施す必要がある。しかし、適切な対策によって防ぐことが可能である。なお、盗聴・改ざん・なりすましに関しては、暗号技術や認証技術での対策が主であり、本稿では取り扱わない。

これに対して、不正アクセスやサービス妨害は、様々な攻撃手段によって、対策をかいくぐる行為であり、防ぐことは困難である。次節では、不正アクセスやサービス妨害を中心に、対策の手法と手順を追いながら、その際に用いられる要素技術について概観する。

2.2 対策のプロセスと要素技術

不正アクセスやサービス妨害について、その手段を大まかに分類すると、

・アカウントの不正取得と悪用
・脆弱性を利用した異常動作発現
・資源の強制浪費
・踏み台による攻撃規模拡大とかく乱

が挙げられる。これに対し、一般の利用者は、

・個々の脅威への対応方針(セキュリティポリシ)の決定
・暗号・認証技術の導入によるデータへのアクセス権限制御
・FireWallやIDS(Intrusion Detection System;侵入検知システム)、ウィルス検査ツールなどの導入によるネットワークへのアクセス制限
・OSやソフトウェアの更新・修正の適用によ

る脆弱性の排除
・セキュリティ監査ツール等によるセキュリティ状況の把握
を行うことで対策する。

一般の利用者が行うこれらの対策は、利用者それぞれの局所的な対策であり、行われている対策のすべてではない。これ以外に、
・プロバイダーなど網レベルでの対応（プロバイダーが行う）
・インターネット自身のセキュリティ能力の向上（機器などのベンダーが行う）
など一般の利用者以外が実施している対策もある。

一般の利用者が対策に利用する、IDSやウィルス検査ツール、セキュリティ監査ツールなどは、既知の攻撃に対して動作するため、新しい攻撃手法が考案されるたびに、攻撃に関するパターン情報等を作成しなければ、対策として機能しない。また、新たな脆弱性が発見されれば、それに対するOSやソフトウェアの修正を作成する必要がある。

つまり、現在の情報通信システムセキュリティ対策は、最新の攻撃に対して対策を立案したり、新たな対策技術を開発したりする側の者がおり、そこで立てられた対策案を基に機器のベンダーやプロバイダーと一般の利用者が対策を実施するという、少なくとも二段階の構造になっている。次節では、このような対策の現状に合わせて、我々の研究を位置付け、本稿での扱いを述べる。

2.3 位置付け

このような観点に基づき、情報通信システムセキュリティに対する研究開発のうち、インターネットセキュリティに対する技術を、
・対策の立案者や新対策技術の開発者を支援する技術
・一般の利用者が対策として用いる技術
の二つに分類し、前者を情報通信システムのセキュリティを確保するための社会基盤と考え「基盤技術」、後者を実際の具体的な対策の技術と考え「対策技術」と呼ぶこととする（図1参照）。

本稿では、我々の研究成果のうち、基盤技術として、

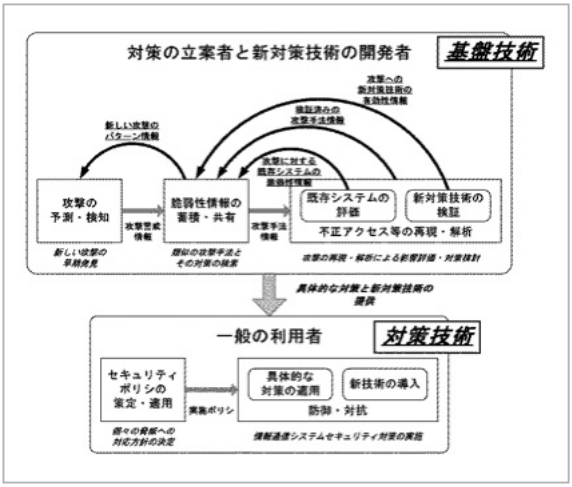

図1 対策イメージと要素技術

・脆弱性情報の蓄積・共有
・不正アクセス等の再現・解析
を位置付け、特に不正アクセス等の再現・解析に関する再現実験環境に重点を置いて述べることとする。

3 脆弱性情報の蓄積・共有

近年の攻撃では、システム固有の脆弱性を利用し、異常動作を発現させることによって、不正アクセスを成功させたり、サービスを妨害したりする脆弱性への攻撃が主な手段となっている。各種のシステムに関して様々な脆弱性が日々発見されており、それらを利用した攻撃手法が次々に編み出されている。

そのため、いち早くシステムの脆弱性に関する情報を把握し、取り除くことが重要である。しかし、脆弱性に関する情報の把握には、
・多数の情報源に散在しているため全情報の網羅が困難
・対策手法の検討に不可欠な情報が非公開の場合が多い
・多くの情報が英語のみで提供されておりローカライズされていない
といった問題がある。

そこで我々は、脆弱性情報を蓄積・整理し、攻撃が発生した場合に既知の脆弱性データに類似情報がないかを検索可能とする「脆弱性情報データベース」[1]の研究開発を行ってきた。この脆弱性情報データベースを、不正アクセス再現実

験装置（**5** 参照）と組み合わせ、脆弱性情報の検証や脆弱性検査まで含めた統合的なセキュリティ対策立案の支援環境を開発し、特許を出願[3]した。

このデータベースには、様々な情報源からの情報を登録可能であり、一般に非公開とされていることが多い脆弱性を引き起こしているソースコードや実際の攻撃ツールの攻撃コードなども同時に登録することができる。また、データの入出力を XML（Extensible Markup Language；拡張可能マーク付け言語）化することで、他のアプリケーションとの連携や独自の検索手法の提供、組織間での情報共有を可能とした。

さらに、脆弱性情報の網羅は困難なため、データベース間の連携は重要である。そこで、我々は、XML を用いた組織間でのデータベースクロス検索を実現する手法を開発し、実際に IPA（Information-technology Promotion Agency、Japan；独立行政法人　情報処理推進機構）脆弱性情報データベース、ICAT Metabase 脆弱性情報データベースと連携させる実証実験を行い、相互に情報の検索が可能となることを確認した。

4　不正アクセス等の再現・解析

不正アクセスやサービス妨害などの攻撃に対する対策を立案したり、防御技術を開発したりする際には、対象とする攻撃の仕組みとその影響に関する情報を入手し、対策が有効であるのかを検証する必要がある。

4.1　不正アクセス等の再現実験環境の意義と目的

不正アクセスやサービス妨害などの攻撃について、その仕組みや影響に関する情報を入手するためには、何らかの方法で攻撃を解析する必要がある。また、対策が有効であるか、悪影響がないかを検証するためには、攻撃に対する対策の効果とそれによる他への影響を測定する必要がある。

解析に関しては、攻撃を実行しているプログラムコードなどが手に入れば、静的にそれを解析することで、攻撃に関する動作については情報を得ることができる。

しかし、その場合でも、脆弱性攻撃などでは一見して攻撃とは思われない動作によって、異常を引き起こさせるため、攻撃対象となっているシステムについて詳細な知識が必要となる。さらには、複数のシステムのうち、どのシステムが対象になっているか不明の場合も多く、その場合には、より広範な知識を必要とする。よって、静的な解析では、実際にどのような作用を与えるかを把握することが困難である。

また、そもそも攻撃を実行しているプログラムコードが手に入らない場合も多くあり、そのような場合には、攻撃によって到達している通信やそれによって引き起こされている現象から、攻撃の仕組みを類推する必要があり、静的な解析では対応できない。

対策の検証に関しては、インターネット上にある各種の情報システムの重要性が低ければ、対策を実際のシステムに施して試行し、問題が発生したら、対策方法を再検討するという緩慢な対応が可能である。

しかし、近年ではインターネットを利用する情報システムの重要性が高まっているため、このような方法で、万が一にも周辺のシステムに悪影響が出た場合には、大きな損害を被る可能性もある。そのため、事前に何らかの方法で対策の有効性と他への影響について、検証しておく必要がある。検証に際しては、システム間の相互作用を把握することが重要であり、これも静的な解析だけでは困難である。

このように、不正アクセス等の解析や対策の検証には、システム間の相互作用に配慮しながら、攻撃や対策によって引き起こされる現象を追跡し、分析できる環境が必要である。このような場合には、関連するシステム全体を模倣し、攻撃を再現し、対策を模擬できるような再現実験環境が有効である。そこで、不正アクセス等の再現解析と対策技術の検証基盤とするため、我々は不正アクセス等の再現実験環境を研究開発してきた。

4.2　不正アクセス等の再現実験環境の要件

インターネット上のセキュリティに関する再現・模擬実験環境には、大きく分けて下記の 6 種類がある。

・トラフィック発生器
　攻撃に関連する特定の通信を発生することで、通信のみを模擬するもの。
・ネットワークシミュレータ
　ネットワーク上の各種の要素をノードとして抽象化し、モデルベースでシミュレートするもの。
・ネットワークエミュレータ
　ネットワークシミュレタに、実際に通信を行うことができる機能などを付加したもの。
・PC やルータのエミュレータで構成した実験環境
　ネットワーク上の主要な要素であるホストとゲートウェイを、PC やルータのエミュレータを用いて模倣する実験環境。
・実 PC やルータで構成した実験環境
　ネットワーク上の主要な要素を、実機で用意し、模擬する実験環境。
・実際のインターネット上に構築した実験環境
　実際のインターネットを用いて実験する実験環境。

これらにはそれぞれ、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手法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手法ほど、規模追従性に富み、実験環境の運用が容易である。

では、セキュリティ事案の分析や対策の策定においては、どのような実験環境が求められるだろうか。

近年のセキュリティ事案の多くは、脆弱性攻撃か DDoS（Distributed Denial of Service；分散型サービス不能）攻撃によるものであり、

・大量の踏み台などを使うため攻撃が大規模
・送信元の詐称など攻撃の仕組みが複雑
・OS やソフトウェアに固有の脆弱性を利用

などの特徴を持つ。

このように、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、影響を測るためには、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。

5　不正アクセス等の再現実験環境

前節で述べたような要件をふまえ、我々は、

・大量の不正な通信を模擬発生できる「不正パケット模倣装置」[4]
・複雑な攻撃の仕組みを実機で再現する「不正アクセス再現実験装置（SIOS）」[1]
・各種の OS やソフトウェアに固有の脆弱性を仮想 PC で模倣する「VM Nebula」[2]

を研究開発した。本節では、それぞれについて概説する。

5.1　不正パケット模倣装置

図2　不正パケット模倣装置

「不正パケット模倣装置」（図 2）は、DDoS 攻撃やワーム等による大量の不正なパケットを模倣し、模擬的に発生することのできるトラフィック発生器である。攻撃者側の挙動は必要なく、攻撃に関連する通信だけ得られればよいような、貫通テストなどに用いることを意図している。

この装置は、トラフィック発生器をベースに開発し、用意したパケットパターンをあらかじめ指定した量や回数などのパラメータに基づいて発生できるようにしたものである。

パケットパターンの作成を可能とする記述言語も開発し、あらゆる種類の不正パケットの発生を可能とした。この装置は、毎秒 48 万パケット送出可能であり、1Gbps の Ethernet 回線を 98.7 %埋める量の不正パケットを生成できることを確認した。

5.2 不正アクセス再現実験装置（SIOS）

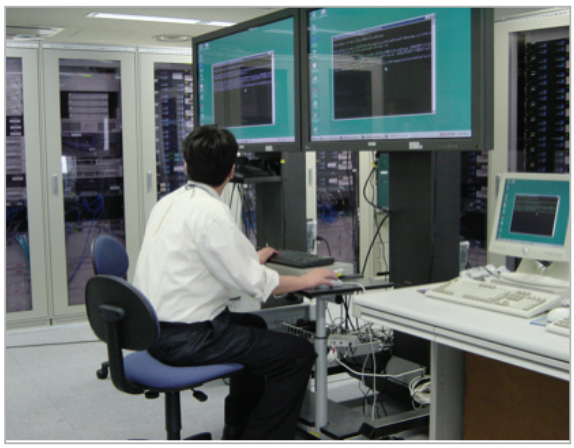

図3 不正アクセス再現実験装置（SIOS）

「不正アクセス再現実験装置」（図 3）は、実機を使って攻撃の正確な再現を可能とした実験環境で、100 台の PC からなる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。

攻撃再現部で実際の攻撃ツールを利用して、送信元の詐称などを含む複雑な攻撃を再現し、インターネット部を介してつながっている被害者部でその影響や脆弱性に関する情報の検証を可能とし、特許を出願[5]した。

一般に、実機を用いる大規模な実験環境では、実験の管理や制御、計測が困難であるが、この装置では、動作条件の設定と自動化を支援するエージェントを組み込むことで、詳細な実験管理を可能とし、特許を出願[6]した。

この装置は、「脆弱性情報データベース」と連携し、攻撃ツールの読み込みや、脆弱性情報の検証が可能であり、さらに、外部の機器を被害者部に接続して実験することにより、各種の機器に対する脆弱性検査を行うこともできる総合的なセキュリティ対策立案の支援環境として開発してきた。さらに、攻撃の予測や検知を行う早期警戒システムとの連携についても研究し、攻撃の早期発見に基づく一貫したセキュリティ対策環境[7]の研究開発を行った。

また、この装置を利用して、実際のセキュリティインシデントを再現し、インシデントに対する対応の演習環境としての機能も研究開発した。この機能を使い、NIRT（National Incident Response Team；内閣官房情報セキュリティ対策推進室緊急対応支援チーム）の演習を試行した。

5.3 VM Nebula

図4 VM Nebula

「VM Nebula」（図 4）は、PC エミュレータによる仮想 PC を使って、一般に使われている OS やソフトウェアがそのまま動作するため、OS やソフトウェアが持つ固有の脆弱性を正確に模倣することができる実験環境である。VM Nebula は、PC エミュレータが動作する数台の模倣サーバとそれらをつなぐマルチレイヤスイッチ、構成の管理を行うライブラリサーバからなる。

脆弱性の検証や攻撃者の挙動解析など、目的ごとに実験環境の構成は変化させる必要があり、実機で構成した場合、物理的な変更が必要になるため、容易ではない。これをシミュレータなどで行った場合には、構成の変化には容易に対応できるが、抽象化されているため、実際の OS やソフトウェア実装の持つ脆弱性などは再現できない。

そこで、VM Nebula では、攻撃者の PC や被害者のサイトのサーバなどの模倣は、すべて仮

想 PC で実現され、それらの間でのネットワーク接続も物理的な接続を変更せずに VLAN で行う。実験系の構成をそのままライブラリサーバに保存、管理し、再実験が必要なときにすぐに読み込んで利用でき、一部を変えて再利用するなど、複数の構成の実験を容易に切り替え可能とした。これにより、実験環境内部に破壊的な影響をもたらすような実験でも容易に再実験可能となり、ウィルスやワームなどの解析に有効であることを確認[8]した。

「不正パケット模倣装置」と「不正アクセス再現実験装置」、「VM Nebula」は、それぞれ性質は異なるが、不正アクセス等を再現し、解析することで、対策を支援するためのものである。そこで、これらの連携についても考察を加え[9]、手法を提案した。連携については、**7** で詳しく述べる。

6　再現実験環境の応用事例

我々は、これまで述べたような不正アクセス等の再現実験環境を用いて、実際に対策技術の研究開発やウィルス・ワームの解析に応用した。本節では、二つの応用事例について述べる。

6.1　抗脆弱性クラスタ

実際に、不正アクセス等の攻撃に対して、セキュリティ対策を講じるためには、FireWall や IDS に代表される防御技術や対抗技術が必要となる。

しかし、これらの技術を導入した多くのシステムが既知の攻撃には対応できるが未知の攻撃には対応できないという問題を持っている。また、Web サーバなど、不特定多数の人にサービスを提供する種々のサーバは、サービスを提供するためにアクセスを公開することが不可欠であり、防御することが困難である。

そこで我々は、未知の攻撃に対して抗う特性を付与した抗脆弱性クラスタ[10]を研究開発した。

「抗脆弱性クラスタ」は、近年の主要な攻撃手段である脆弱性攻撃に対応するため、攻撃を受けたと判断した場合、OS やサービスソフトウェアを自動で切り替えるクラスタである。

脆弱性は OS やサービスソフトウェアごとに固有であるため、ある脆弱性攻撃が有効な OS やソフトウェアは限られている。そのため、その脆弱性を持たない別の OS やソフトウェアで動作しているシステムには、影響がない。脆弱性クラスタはこの特性を利用して、脆弱性攻撃の無効化を図る。

このようなクラスタについて、公開サービス用のサーバに利用することを目指し、仮想マシン技術を応用して、抗脆弱性サーバシステムを開発[11]した。

抗脆弱性クラスタを研究開発する際には、実際にシステムにとって未知の攻撃が飛んできた場合に、有効に機能するかどうかを検証する必要がある。そこで、VM Nebula を用いて、実験環境内部に攻撃ホストと抗脆弱性クラスタを用意し、未知の攻撃を模擬することで、抗脆弱性クラスタがどのように動作するのかを確認した。

6.2　MS.Blaster ワームの解析

ウィルスやワームを解析する際には、感染経路とその手段、対象と残される痕跡、感染後の動作と影響などを調べる必要がある。これらを解析するためには、ウィルス・ワームのプログラムコードから静的な解析が行われる。しかし、動作が複雑なウィルス・ワームの場合、静的な解析だけでは、十分な情報を得られないため、実際にウィルス・ワームの検体を動作させて解析する動態解析と組み合わせて行うことが多い。

動態解析を行う場合には、実際に感染動作をさせる必要があるため、ウィルス・ワームの流出を避けるために、解析用の隔離された実験環境で行われる。ウィルス・ワームの解析には、特定の脆弱性を再現できる必要があるため、実機と同程度の再現能力が、実験環境に求められる。ウィルス・ワームを解析するためには、検体に感染動作を実行させ、実際に感染させる必要があり、対象となった実験環境内の PC などは感染状態となる。しかし、ウィルス・ワームの解析と検証を一度の感染動作の再現で行うのは困難であるため、一度感染させた後に、非感染状態に戻し、再度実験を行うといった再実験が不可欠である。

実機を用いた環境では、この際に OS やアプリケーションソフトウェアを再度インストール

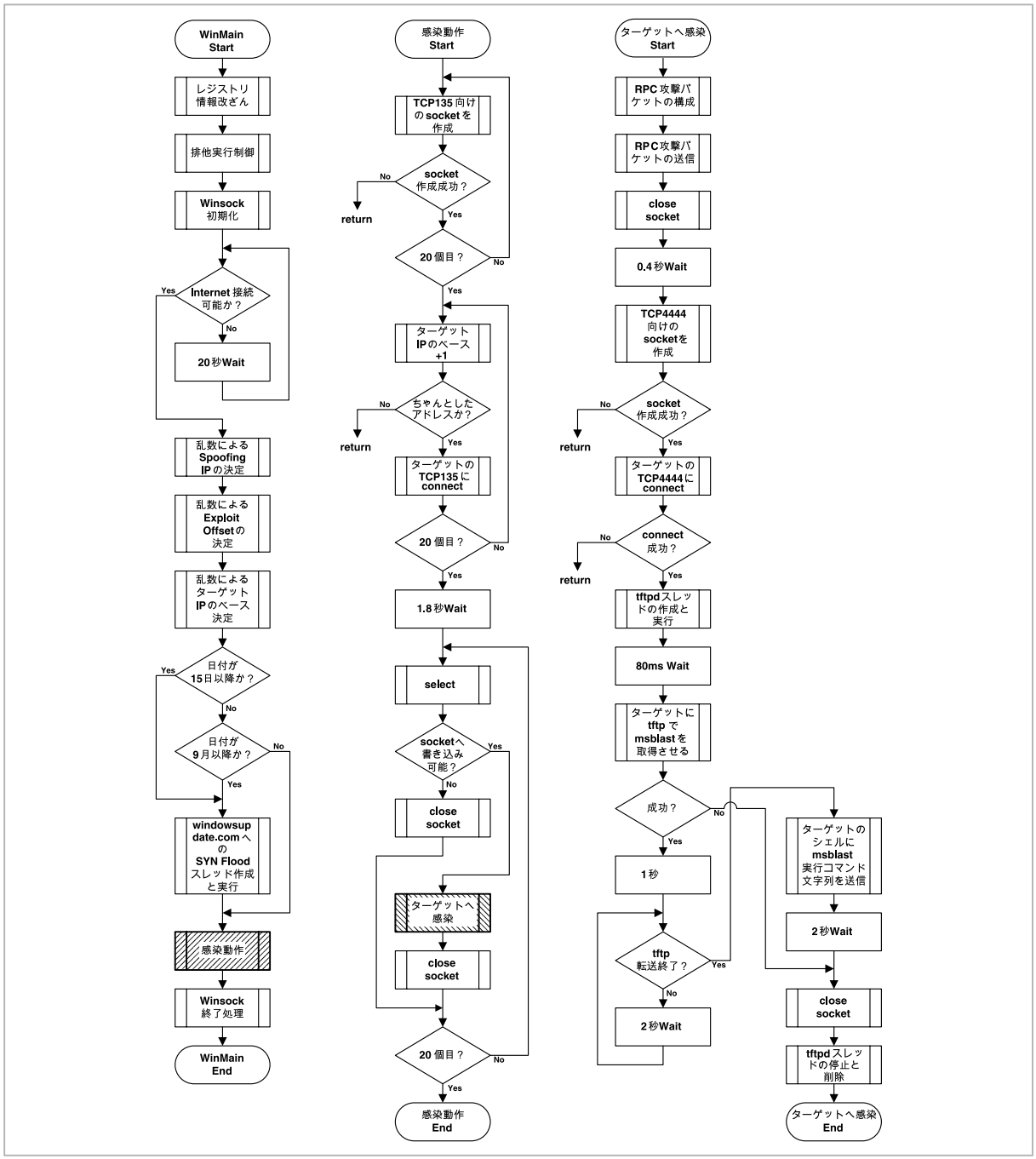

図5 MS.Blaster ワームの動作フローチャート（解析結果）

し、設定し直す必要があり、大きな工数がかかる。

これに対して、VM Nebula では、実験環境を作った後、非感染状態でその環境をライブラリに保存しておけば、感染状態になったとしても、保存してある実験環境を読み込むだけで、すぐに再実験が可能となる。

これを用いて、何度も感染状態から非感染状態へ戻す必要があるため通常は困難な、ウィルス・ワームの動態解析について、実際に MS.Blaster ワームを解析（図 5 参照）[8] し、その有効性を確認した。

7 単一の実験環境の限界と複数の実験環境の連携

これまで、不正アクセス等の仕組みの解析や対策技術の有効性や影響の評価に用いる再現実

験環境について述べてきた。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、単一実験環境での再現は困難となってきている。

そこで本節では、単一の実験環境の限界と複数の実験環境の連携について述べる。

7.1 単一の実験環境の限界

実験環境には様々な種類があり、それぞれに得手不得手がある。また、その実装によって規模や構成は制約される。実験環境は、ある特定時期の事案の状況に合わせて構築されるのが一般的である。そのため、実験可能な規模や再現の対象は、設計時の状況に合わせて設計され、固定である。しかし、実際には事案の状況は変化しており、実験環境の構成を変更せねば対応できない。

ネットワークシミュレータやエミュレータであれば、規模の拡大は、内部のノード数の増加のみで対応できるため、特にコストを必要とせず、ある程度まで許容することができる。しかし、実機で構成された実験環境等の場合には、規模の拡大は、そのまま実際のノードの追加を意味することが多く、大きなコストを必要とする。

また、実機で構成された実験環境等では、再現対象の変更は、多くの場合、各ノードのOSやソフトウェアの変更で対応できる。しかし、ネットワークシミュレータやエミュレータの場合は再現対象を変更する場合には、それ自体の実装を作り直す必要があり、求められる対象によっては再現することは非常に困難となる。

以上のように、単一の実験環境では、セキュリティ事案の状況の変化に対応することは困難である。そのため、事案の状況変化に合わせて大きなコストが必要となる。

7.2 複数の実験環境の連携

前節で述べたように単一の実験環境では、その再現、模擬の能力は設計時に想定された限界がある。しかしながら、セキュリティ事案の状況の変化に合わせて、その限界を超えた能力が要求されるようになる。その際に、無尽蔵に大きなコストを費やすことができれば、状況に合わせた変更が可能であるが、実際には、コストは最小限に抑えることが要求される。

そこで本節では、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。

実験環境を連携させることで、例えば以下のようなことが実現できると考えられる。

- 100ノードと500ノードからなる実機による実験環境同士を接続して、全体で600ノードに規模を拡大する。
- 実機とネットワークエミュレータを連携させ、再現性能と規模追従性の両方の向上を図る。

しかし、連携といってもただつなげば、実験環境として機能するわけではない。特に、インターネットセキュリティに関する実験に使う場合には、通信が相互にやりとりできる必要があると考えられる。また、通信だけではなく、計測・記録した情報についても、やりとりできる必要があるだろう。さらに、それぞれの環境がバラバラに動作するのではなく、イベント単位や時間単位で連動する必要がある。特に、通信に対する応答などは、互いに正しい順序で発生しなければならないと考えられる。

このように、複数の実験環境を連携させる上で、接続の手法やどのように連携させるのか、実験環境間の様々な違いをどうするのかなど[12]検討すべき問題が幾つかある。

7.3 実験環境連携の試行

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下記の三つの実験環境の連携実験[13]を事例として取り上げる（図6参照）。

- 不正アクセス再現実験装置（SIOS）（**5.2** 参照）
- VM Nebula（**5.3** 参照）
- StarBED[2]

これらの三つの実験環境は、互いに地理的に離れたところに設置されている。そのため、接続を行う物理回線が必要であり、また、相互に操作を実現するような何らかの遠隔操作手段が必要であった。

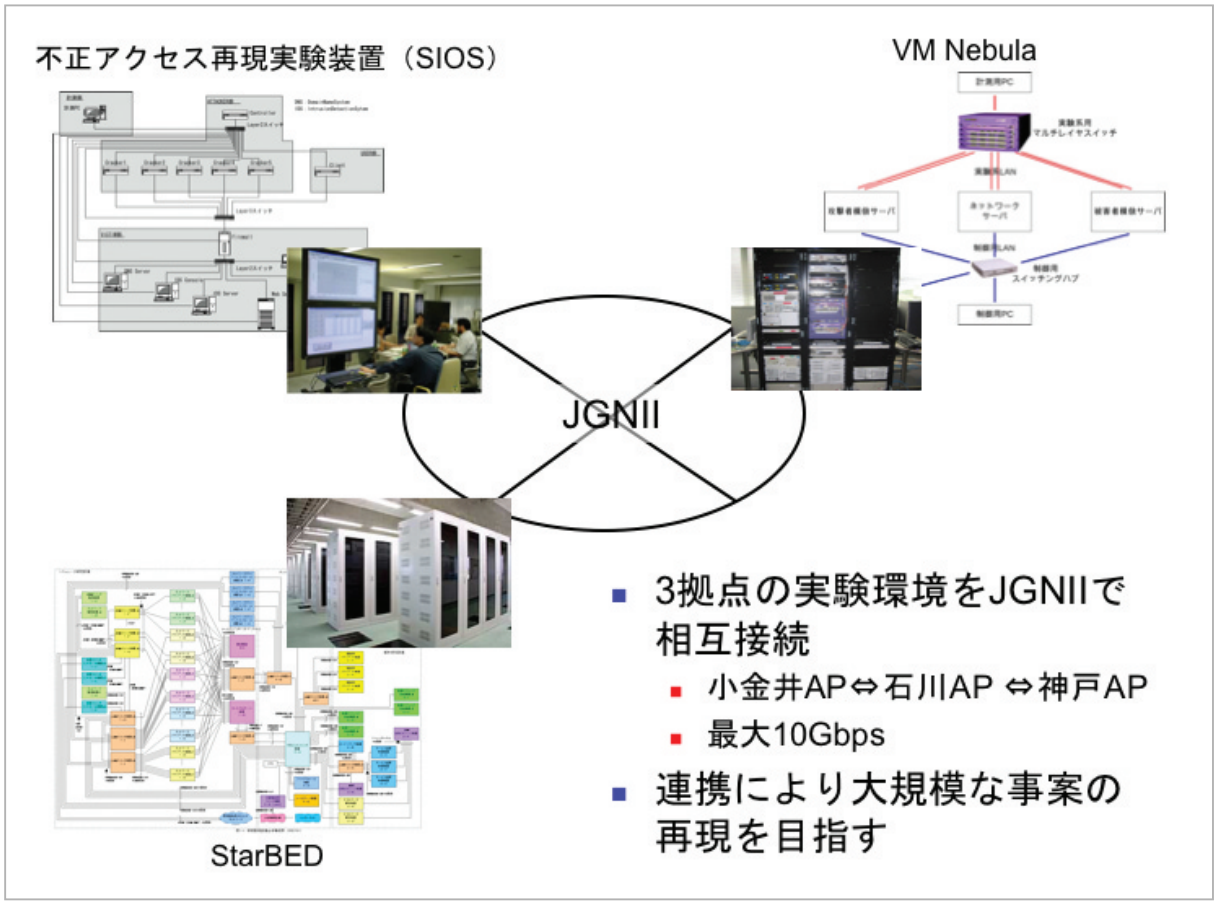

図6 三つの実験環境の連携

物理接続に関しては、専用回線のみによる接続、所内共用の広域 LAN と専用回線の組合せ、JGN2 を利用した接続の三つの案の中から JGN2 による物理接続を行うこととした。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 JGN2 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、JGN2 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[3]利用する。SIOS（東京都小金井市）とStarBED（石川県能美市）の間は、10Gbps で、VM Nebula（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

論理的な接続については、それぞれの実験環境で、プライベート IP アドレス空間を固有のルールで利用しているため、IP アドレスの割当やルーティングの有無、ルーティング方式について取決めを行う必要がある。また、各実験環境のどの部分とどの部分を接続するのかといったトポロジとその部分での出入りの方式なども検討を行わねばならない。

遠隔操作手段としては、まずは、各実験環境に既設の KVM over IP 装置があるため、当面はこれを利用し、それぞれの環境から実際に画面を見ながらキーボードやマウスを遠隔操作することとした。ただし、これでは運用管理が困難であるため、統一的なインタフェイスの用意などを実施する予定である。

なお、今回対象とする実験環境は、すべて、

実際のOS実装とソフトウェア実装を用いて実時間ベースで動作する。よって、今回はNTPによる時刻同期は予定しているが、同期の手法には検討の余地がある。また、それ以外には今回は、これらを接続する上では、特別な仕掛けを用意することはしていない。

執筆時点で、この連携実験に関しては準備中であり、接続後の状況に関しては機会があれば、別途報告したい。

2　StarBEDは情報通信研究機構北陸IT研究開発支援センター（石川県能美市）に設置されているシミュレータ施設の愛称で、512台のPCからなるネットワーク関連実験用の汎用クラスタである。
3　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いただけることとなった。VLANの張り替えは手動で行う。

8　まとめ

本稿では、インターネットセキュリティ上の脅威に対抗するための技術開発の基盤となる、不正アクセスなどの再現・解析を行う実験環境について、我々が研究開発してきた再現装置や実験環境について述べ、連携の検討を示した。

今後は、インターネット全体の要素を考えた根本的な対策を検討できるような、大規模かつ複雑な事案を取り扱える実験環境を作るにはどうすればよいのかを検討するとともに、その実験環境を使って更に新たな対策技術などの研究開発を進めていきたいと考えている。

参考文献

1　大野浩之，武智　洋，永島秀樹，“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　横地　裕，山本　泉，武智　洋，永島秀己，大野浩之，“脆弱性検査システム”，特許出願2001-21406，特許公開2002-229946，Jan. 2001.
4　三輪信介，滝澤　修，大野浩之，“トラフィックジェネレータによるDDoS攻撃の再現”，情報処理学会　マルチメディア通信と分散処理研究会コンピュータセキュリティ研究会　合同研究会，Feb. 2003.
5　大野浩之，五百蔵 聡，永島秀己，武智　洋，“コンピュータ・システムの脆弱性検査システム”，特許出願2001-21404，特許公開2002-229945，Jan. 2001.
6　大野浩之，武智　洋，永島秀己，柳橋宏樹，久保和也，“分散環境における動作条件設定方法及びこれを用いたシステム”，特許出願2001-21405，特許公開2002-229877，Jan. 2001.
7　三輪信介，大野浩之，“早期発見に基づく一貫したインターネットセキュリティ対策環境”，電子情報通信学会，2002年暗号と情報セキュリティシンポジウム（SCIS2002），Jan. 2002.
8　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.（IC2003論文賞受賞）
9　三輪信介，“不正アクセス等再現・模倣実験環境の統合に関する一考察”，情報処理学会　マルチメディアと分散処理2003年ワークショップ，Dec. 2003.
10　三輪信介，“抗脆弱性クラスタの設計と実装”，日本ソフトウェア学会　WIT2003，Nov. 2003.
11　三輪信介，“抗脆弱性サーバシステムの設計―Virtual　Machine技術の応用―”，日本ソフトウェア学会WIT2001，Sep. 2001.
12　三輪信介，大野浩之，“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”，情報処理学会，マルチメディアと分散処理2004年ワークショップ，Dec. 2004.
13　三輪信介，宮地利幸，大野浩之，篠田陽一，“不正アクセス等再現実験環境の統合手法に関する研究”，電子情報通信学会，2005年　暗号と情報セキュリティシンポジウム（SCIS2005），Jan. 2005.

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