ミクロな分析技術の動向

2

篠田陽一 （独）情報通信研究機構（NICT）

ミクロ分析とは

政府系のWebサイトや特定企業のサーバを狙ったサイバー攻撃をはじめ，日々大量に届くスパムメールやフィッシングメール，WinnyやShareなどファイル交換ソフトを介した情報漏えいなど，インターネットで生起しているセキュリティ・インシデント(セキュリティ事故)や迷惑行為の多くは，ウイルスやワーム，ボットといった不正プログラムに感染したコンピュータによって引き起こされている．このような不正プログラム，および不正プログラムがネットワークを経由して感染を拡大する際に使用する攻撃コードを併せて不正コードと呼ぶこととする．不正コードを収集し，それらを分析することは，情報通信インフラに対する脅威の根本原因のメカニズムを解明し，そこから有効な対策を導出するという意味においてきわめて重要であり，これら不正コードに対抗するための精緻で微視的な技術を総称してミクロ分析と呼ぶ．

ミクロ分析は大きく，攻撃情報の収集，不正コードの検出，不正コードの分析の3段階に分けることができる．攻撃情報の収集には，ハニーポットと呼ばれる，脆弱なシステムを装った囮サーバを用いる場合が多い．ハニーポットの設計・構築においては，攻撃をおびき寄せるための偽装技術が重要であることは言うまでもないが，攻撃を受けた際に実際的な被害の発生を抑制し攻撃情報を収集する技術が要求される．このため，脆弱なサービスやシステムをエミュレートしたり，仮想化技術を用いる手法なども検討されている．

不正コードの検出では，従来からシグネチャマッチングによる検出が広く行われてきた．しかしながら，新種の不正プログラムの出現頻度が上昇し，またシグネチャによる検出を回避するための自己改変機能を持つ不正プログラムが登場するなど，シグネチャマッチングの有効性は低下している．そのため，プログラムの構造を高速で解析し，不正プログラムを検出する技術や，仮想環境における振る舞いを観測することでプログラムの悪性を判断する技術が重要となる．

不正コードの分析では，リバースエンジニアリングの手法を用いて不正プログラムを人間可読なレベルにまで還元し，その挙動や特徴を分析する静的解析と呼ばれる手法や，不正プログラムを隔離された実験環境において実行し，そのネットワーク的挙動や感染ホスト内部での挙動を詳細に抽出する動的解析と呼ばれる手法が存在する．また，不正プログラムの活動がネットワークに及ぼす影響を調べるために，ネットワークシミュレーションやネットワークエミュレーションを用いて不正プログラムの感染や攻撃の再現を試みる技術も重要である．

平成16年度に開始された文部科学省科学技術振興調整費プロジェクト「セキュリティ情報の分析と共有システムの開発」においても，上記のミクロ分析の3段階についてそれぞれ研究開発を行った．以降では，その概要を紹介する．

「セキュリティ情報の分析と共有システムの開発」プロジェクトにおけるミクロ分析

文部科学省科学技術振興調整費によるプロジェクト「セキュリティ情報の分析と共有システムの開発」におけるミクロ分析について紹介する．各研究テーマの関係については図-1を参照のこと．

まず京都大学が担当した「不正コード収集技術に関する研究」では，OSやサードパーティ製品に対する攻撃情報の収集を有効的かつ効率的に行うハニーポットシステムを構築し，多数の脆弱性やゼロデイ攻撃を早期に検知し，攻撃に関する多くの知見を得た．(株)セキュアウェアが担当した「不正コード検出・解析技術に関する研究」では，「不正コード収集技術に関する研究」と密に連携し，上記ハニーポットにより収集された攻撃情報から，シェルコード（ソフトウェアの脆弱性を攻撃し，制御を奪う機械語プログラム）を検知するシステムを構築すると

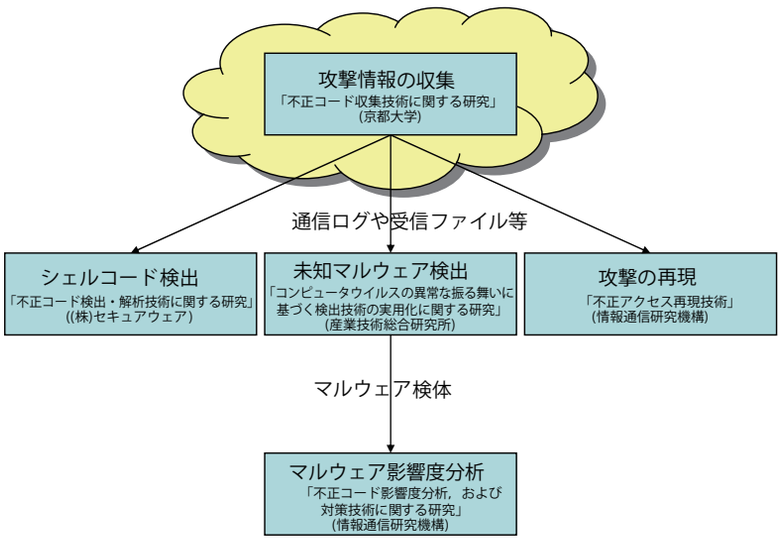

図 -1 インターネット上の攻撃情報分析システムにおけるミクロ分析の概要

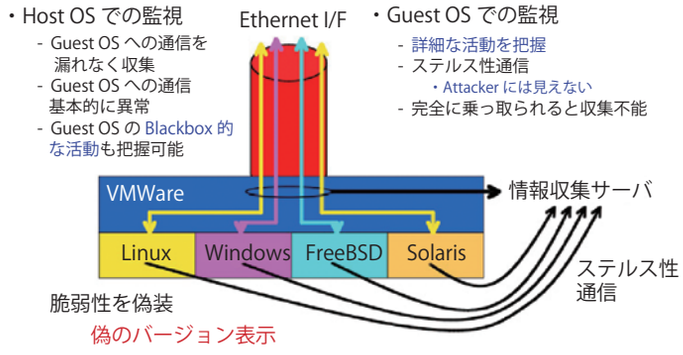

図 -2 偽装サーバの構成

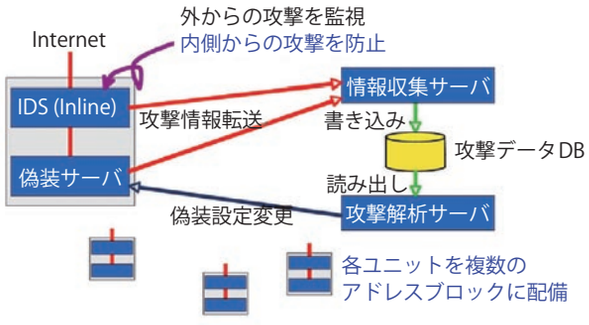

図 -3 偽装サーバシステムの構成

ともに，検出手法のさらなる高精度化，およびハードウェア実装による高速化に取り組んだ．産業技術総合研究所が担当した「コンピュータウイルスの異常な振る舞いに基づく検出技術の実用化に関する研究」では，ハニーポット等で収集された実行ファイルを解析し，外部 API ライブラリ関数の呼び出しレベルでの不正な振る舞いを検出することで，未知のマルウェアを高精度で検出する手法を確立するとともに，メールサーバ等へ検知ツールを組み込み，実環境での評価を行った．情報通信研究機構が担当した「不正アクセス再現技術」では，ネットワーク攻撃を大規模環境で再現するため，地理的に離れた 3 つの再現実験環境を接続し，さらに実験管理機能の統合を行うことで，大規模なネットワーク攻撃の実証模擬実験を行った．同様に情報通信研究機構が担当した「マルウェア影響度分析」では，ハニーポットで収集された不正プログラム(マルウェア)を仮想環境で実行し，その観測結果とナレッジデータベースに基づき自動的にネットワーク上での対策を導出・検証するシステムを構築した．

■不正コード収集技術に関する研究

本研究テーマでは，不正コードによる管理者権限奪取を防止しながらも，OS 等の脆弱性を偽装する偽装システムを試作し，京都大学をはじめとする協力機関のネットワークに配備して不正コードの収集を行った[1)]．攻撃情報を収集するために構築したシステムを以下に説明する．まず，平成 16 年は，VMWare 等の仮想システム上に OS を多数搭載し，各 OS 上で Web，メール等の一般的なサービスを稼働させる偽装サーバを構築した（図 -2）．OS 本体，あるいは，サービスプログラムへの通信で，RPC に準拠しないセッションデータを検知した場合は，セッションデータをファイルとして保存し，他サブテーマでの解析が行えるようなシステムを構築した(図 -3)．

観測結果から，仮想システム上で稼働していることを察知し回避する攻撃，逆に意図的に効果のない不正コードを多用する攻撃が存在することが判明した．

また，Microsoft Windows 系のグラフィクス処理関数の脆弱性を狙った攻撃（MS06-001）に関しては，この攻撃の検知には，罠が仕掛けられている Web サイトへブ

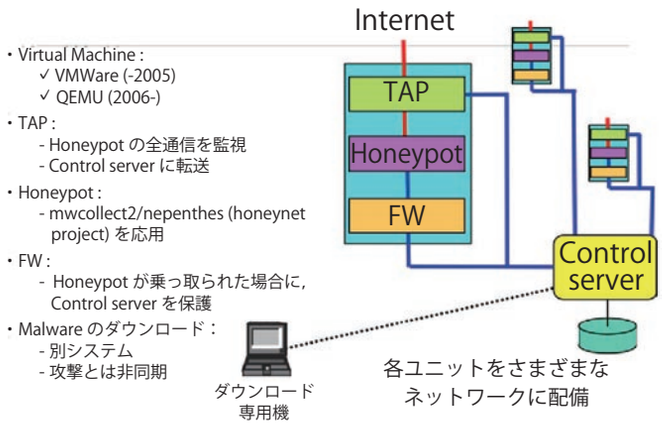

図 -4　サードパーティ製品への攻撃情報収集システム

ラウザでアクセスしなければならない．このため，通常は受動的に不正コードを受信するだけの偽装サーバの構成を一部変更し，能動的に Web アクセスを行う改造も施した．

平成 17 年度は前年度の観測結果を受け，仮想システムを用いず，実マシン上に OS を搭載した偽装サーバを構築した．パッチを適用していない OS を用いるため，管理者権限奪取に備え，偽装サーバの通信を強制遮断するシステムを開発した．また，「不正コード検出・解析技術に関する研究」と連携することにより，不正コードによる攻撃状況の可視化システム，および，不正コードの半自動解析システムの開発を行った．さらには，研究テーマ「不正コード収集，検出・解析，および対策技術」内での，連携研究を開始し，観測データの提供，および，共同解析を行った．

平成 18 年度は，それまでの観測結果に基づき，OS 以外の脆弱性に対する攻撃も追跡する必要があると判断し，サードパーティ製品への不正コードを収集することを目標とした．この目標を達成するため，図 -4 に示す通り，TAP，Honeypot，FW の 3 モジュールから構成されるユニットを分散配置した．TAP は Honeypot に対するアクセス情報の収集を目的とし，FW は万が一 Honeypot が乗っ取られることがあっても，指示を出す Control server および制御用回線（青線）の存在を遮蔽することを目的としている．

このように，平成 19 年 3 月 31 日までに，重複を除く 44,011 個の IP アドレスから攻撃を受け，延べ 569,778 件の不正コードを収集した．その内訳は，559,897 種類の不正コードであり，不正コードに使用されたシェルコードは 272 種類であった．このことから，不正コードは頻繁に改良が試みられているが，攻撃の要であるシェルコードは少数のものが流用されていることが分かった．また，1 つの脆弱性（MS06-040）については，50 種類以上のシェルコードが試されながらも，管理者権限が奪えるものは 1 種類のみであること，さらには，その 1 種類を用いても，管理者権限の奪取率が 90% 程度にとどまることなどから，最近のオペレーティングシステムの頑強性を示す結果となった．

さらに，allaple と呼ばれるマルウェアによるゼロデイ攻撃を，セキュリティ研究者のメーリングリストで話題になる 2 カ月以上前に検知し，JPCERT/CC へ報告を行うことに成功した．このほかに，オープンソースソフトウェアである samba および商用アプリケーションである Symantec 製品に対するゼロデイ攻撃も検知した．なお，後者については，JPCERT/CC による警報発表の根拠データとして活用されたと聞いている．また，既知のマルウェアに偽装した不正コード開発活動や，偽装サーバ等の観測システムに対する逆探知活動なども検知した．上記の成果を得るための偽装サーバについては，管理者権限を奪われることは一度もなかった．このため，管理者権限を奪取された場合の状況を調査した．Unix 系の偽装サーバ 1 台に対する辞書攻撃を許し，実際に乗っ取りを行わせることに成功した．その結果，Unix 系システムを乗っ取った場合，そのネットワーク環境を数カ月に渡って精査し，その後，当該システムへの不正アクセス方法を他人に譲渡したと推定される結果を得た．

■不正コード検出技術に関する研究

シェルコード検出技術：不正コード検出・解析技術に関する研究

本研究テーマでは，平成 16 年度から平成 18 年度にかけて，前節で述べたハニーポット（偽装サーバシステム）からの最新の不正コードを収集・解析した．平成 18 年 7 月には Windows に対する未検知の攻撃コードを発見したが，この攻撃コードを検知するべく，不正コード検知アルゴリズムに改良を加えた．現時点での不正コード検知アルゴリズムは，現時点までにハニーポットから収集した不正コードをすべて検知可能である．現時点までにハニーポットから収集した不正コードの総数は，200 種類以上，個数としては 20,000 個以上に及ぶ．

また，平成 16 年 4 月から平成 19 年 3 月にかけて，インターネット上で入手可能なシェルコードを収集し，解析を行った．収集したシェルコードは計 385 個であった．

さらに不正コード検知アルゴリズムのハードウェア化を目指したアーキテクチャ設計を行った．アーキテクチャ設計においては，TCP/IP データストリーム再構築部と攻撃コード検知部を分離し，独立に動作できるように設計した．さらにこの設計に基づいた詳細設計を行った後，HDL を用いて直接にハードウェアコーディングを行った結果，700Mbps 以上の処理速度を得た．

コンピュータウイルスの異常な振る舞いに基づく検出技術の実用化に関する研究

本研究テーマでは，以前から産総研において開発を行ってきた未知ウイルス検知ツールをベースとし，その効率化と洗練化を通じて，数百名規模のユーザを持つメールサーバをウイルス攻撃から堅牢に防御するための実用技術の確立を目的に研究開発を行った[2)]．

本研究のベースとなった未知ウイルス検知システムは，IA32 アーキテクチャ上の Win32 プラットフォームで動作する実行ファイルを対象に，プログラムコードを動的かつ静的に解析することで，外部 API ライブラリ関数の呼び出しレベルでの悪意ある振る舞いを検出し，あらかじめ定義された禁止すべき振る舞いと突き合わせ，当該実行ファイルがワーム／ウイルスであるかどうかを判定するものであった．システムは，(1) 自己解凍・変形ウイルス／ワームへの対応のための CPU シミュレータ，(2) 振る舞い解析のための軽量 OS エミュレーション機能，(3) 禁止すべき振る舞いの定義と検知を行うポリシー処理系，(4) コード先読み処理のための静的解析部，からなり，実行される可能性のあるすべてのコードを解析することが可能になっている．しかし，実用化を考えた場合，(1) 検知ポリシー（検知すべき悪意ある振る舞い）の定義に汎用性が欠ける，(2) 実用に耐え得るポリシーセットが用意されていない，(3) 軽量 OS エミュレーションのための仮想実行環境の不足による検知漏れの顕在化，(4) 実環境におけるサーバへの組み込みモジュールの不足，(5) 被害が拡大化しつつあったボットネットワームへの対応の切実化，などの課題があった．本プロジェクトでは，これらの課題に対処して検知ツールの実用性を向上させた．

具体的には，プログラムの悪意ある振る舞いを定義するポリシー定義言語を設計し，この言語による記述をシステム上で実行可能なプログラムコードに変換するマクロ処理系の実装を行った．これにより，ポリシー処理系が検知システム中のコードシミュレータから独立して稼働するよう改善された．また，ウイルス検知のための仮想実行環境において，ライブラリ関数を処理するためのスタブ関数を自動生成するためのツール，およびレジストリやファイル構成や環境変数を格納するデータベースの作成を行った．公開されているライブラリ情報からスタブ関数の雛形と仮想ライブラリファイルを自動生成することで，エミュレーション性能が劇的に向上した．同時に，継続的なワーム／ウイルスサンプルの収集と解析を通じて，スタブ関数において必要なエミュレーションコードの実装とその他の仮想実行環境の整備を行い，当該年度までに捕捉・蓄積されたウイルスを検知するのに十分な仮想実行環境を整備することができた．

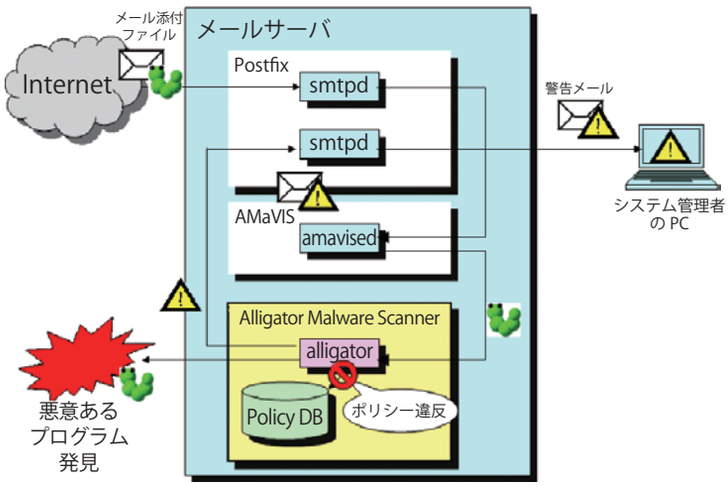

図 -5 サーバ組み込みモジュールの動作（メールサーバ）

また，実環境におけるサーバ上で検知ツールを用いた運用を可能にするためのツール統合を行った．具体的には，メールサーバ（図 -5 参照）や Web プロキシサーバを検知ツールと連携させ，悪意ある振る舞いを示す実行ファイルが検知された場合に必要な警告処理等を行うサーバ組み込みモジュールを開発した．これらの組み込みモジュールによる検知ツールの試用で得られた知見に基づき，将来予見されるウイルスに対して有効と考えられる汎用ポリシーセットを 20 個程度のポリシーにより定義した．具体的には，自己コピー，不正ファイルアクセス，外部プログラム／プロセス実行，レジストリ書き換え，大量メール送信，ソケット通信，対デバッガ／エミュレーション，不正アドレス実行，プロセス走査，ファイル走査などの汎用ポリシーを定義し，これまでに収集されたサンプルに対する検知試験を行い，その有効性を確認した．これにより，メールサーバについては数百人規模のユーザを対象とした未知ワーム／ウイルス検出の実験が行えることが確認できた．

次に，上記検知ツールを，実環境においてメールサーバやプロキシサーバと連携させ，検知性能や処理効率の評価を行いツールの改善を行った．また，実稼働しているメールサーバで捕捉された実行可能ファイルをオフラインで検知ツールに渡し，悪意あるものかどうかを検査する実験をほぼ 1 年通じて行った．評価として，既存のアンチウイルスツールによる事後の検査と照合し，結果として平成 18 年度中（4 月から 2 月）にメールサーバ上で捕捉された約 150 個（重複除く）のウイルス／ワーム（IA32 プラットフォーム上の Win32 実行可能ファイルに限り，また Visual Basic や .NET の中間言語コードによるものを除く）について，当初目標であった未知状態での検知率 95% 以上を達成した．

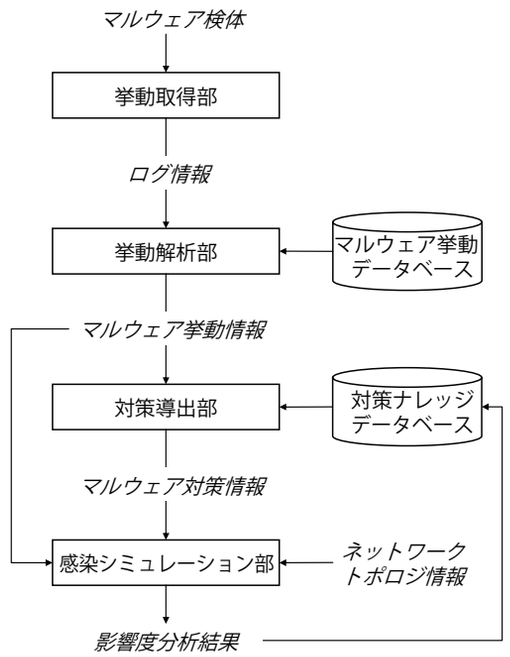

図 -6　マルウェア影響度分析システムの処理の流れ

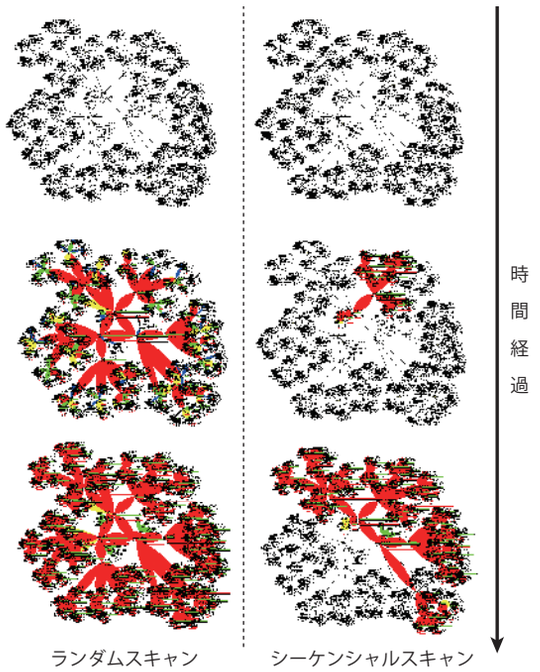

図 -7　ランダムスキャン（左）とシーケンシャルスキャン（右）の様子

他方で，メール添付型のワーム／ウイルスは沈静化してきており，いわゆるボットネットを形成するためのワームによる被害が深刻化してきた．そのため，オープンソースで利用できるハニーポットツールを用いて捕捉される実行可能ファイルを即座に検知ツールに渡す組み込みモジュールを開発し，実環境で実験を行うことができた．実験を行ったのは平成 19 年 2 月から 3 月にかけてであったが，この間に囮サーバで捕捉されたボットネットワーク 10 数個（重複除く）についてリアルタイムで悪性を検知するとともに，約半数については，制御用接続の IP アドレスとポート番号の情報を自動的に取得することができた．また，乱数に関する API 関数をエミュレートすることにより，新規感染動作対象となる IP アドレス分布についてのおおまかな情報を取得することが可能であることが分かった．

■不正コード影響度分析，および対策技術に関する研究

本研究テーマでは，コンピュータウイルス，ワーム，ボットなどの不正コードの挙動や感染・伝播の様子を分析することで，それらの不正コードがネットワークに与える負荷の観点から影響度分析を行うとともに，当該影響を極小化するための対策を自動的に導出する研究を実施した．具体的な研究成果としては，不正コードの影響度分析および，対策の自動導出・検証を行う「マルウェア影響度分析システム」を構築し，実際の不正コードに対する影響度解析実験および対策導出実験を行った [3]．

図 -6 にマルウェア影響度分析システムの処理の流れを示す．マルウェア影響度分析システムは，4 つの機能部と 2 つのデータベースからなっている．挙動取得部では，入力されたマルウェア検体を仮想マシン上で実行し，ファイルアクセス，レジストリアクセス，外部との通信のログを収集する．挙動解析部では，マルウェア挙動データベースに記述された挙動パターンに基づき，挙動取得部で得られたログ情報からマルウェアの挙動を抽出し，マルウェア挙動情報として出力する．次に対策導出部では，対策ナレッジデータベースに記述された，マルウェアの挙動と対策の対応関係に基づき，挙動解析部が出力したマルウェア挙動情報に対して有効なマルウェア対策情報を導出する．最後に，感染シミュレーション部では，マルウェア挙動情報，マルウェア対策情報，ネットワークトポロジ情報を基に，マルウェアのネットワーク感染の様子をシミュレートし，該当マルウェアの影響度を測定する．さらに，導出された対策をシミュレーションに反映することで，対策の効果を測定する．

図 -7 はそれぞれランダムスキャンとシーケンシャルスキャンを行う仮想マルウェアの感染の様子を感染シミュレーション部により模擬した結果である．図中で，マルウェア感染により発生した通信は赤く表示されている．ランダムスキャンではネットワーク全体に一様に不正コードが拡散していくが，シーケンシャルスキャンでは近くのサブネットから感染が広がっていく様子が確認できる．この例では，シーケンシャルスキャンよりランダムスキャンの方が急速に感染台数を増加させていった

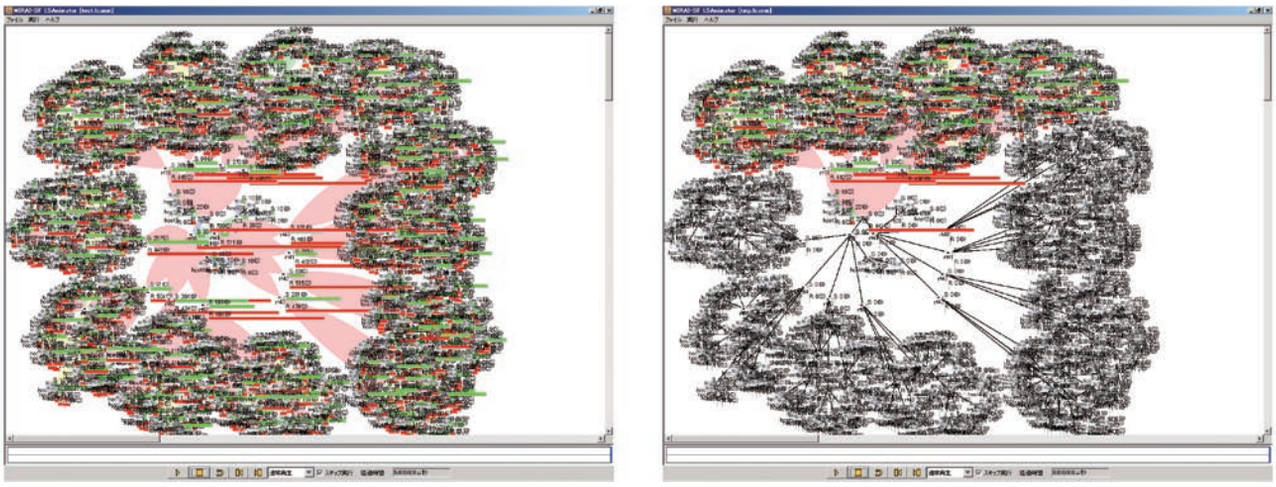

図 -8 対策前後のウイルス拡散の様子（左は対策前，右は対策後）

様子が確認できる．今回の例では，ランダムスキャンの方が感染拡大の速度が速かったが，仮想ネットワークに設定するパラメタによって結果が異なってくる．たとえば，ランダムスキャンによってアクティブなホストに到達する可能性や，サブネットワーク中の何％のマシンが不正コードに対する脆弱性を持つか，などを設定することが可能である．実際のシミュレーションでは，複数のプロバイダの接続関係を考慮したネットワークトポロジや，各プロバイダ内でのセキュリティパッチの配布状況などの情報を可能な限りパラメタに反映させることにより，より正確なシミュレーションを行うことが可能になる．

次に対策導入前の不正コード拡散のシミュレーション結果を図 -8 左に示す．これに対して対策導出部において，サブネットワークを中継する位置にあるルータに対するパケットフィルタの対策を自動的に導出し，対策適用後の不正コード拡散のシミュレーションを実行することが可能である．対策導入後のシミュレーションを図 -8 右に示す．不正コードの拡散があるルータを境界にして防御されていることが確認できる．対策前と対策後の不正コード感染ホスト台数の差により，その対策による改善度を算出する．対策導出システムは，複数の対策手順を導出した場合には，改善度によって優劣を判定し，対策を適用する際の優先度として設定する．このような対策手順は，データベースに蓄積されたナレッジを利用して自動的に導出することが可能であり，不正コードの被害が広がりつつある際に，推奨される対策案を複数作成し，それぞれに優先順位を付与してネットワーク管理者に提示する，などの運用を想定している．

■ミクロ分析関連技術：不正アクセス再現技術

本研究テーマでは，複雑化・広域化の一途をたどる不正アクセスの正確な分析を目指し，この再現・模擬・模倣実験に必要な，複数の再現実験環境を連携・統合させる手法について，不正アクセス等の再現実験環境の連携実験テストベッドを構築し，統合手法の検討を行い，プロトタイプシステムを作成し，統合実験用評価コンテンツを用いて実証実験を実施した[4]．これにより，複数の実験環境を連携・統合させる上での問題点と利点を明らかにし，実際に複数の再現実験環境を連携・統合させることで既存の実験環境では再現困難な事案の再現が可能となることを確認した．以下では，その概要を説明する．

まず，実験環境の連携について検討するために，NICT 小金井本部の不正アクセス再現実験装置（呼称 SIOS），NICT 関西先端研究センターの VM Nebula，NICT 北陸 IT 研究開発支援センター（現 北陸リサーチセンター）の研究設備 StarBED の 3 つの実験環境を用いて，再現実験環境の連携実験テストベッドを構築した（図 -9）．これらの 3 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る．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 3 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利用する．初期の状態では，各実験環境の操作は独立しており，すべての割り当て・設定作業，実験遂行の制御も独立して行われている．統合手法としては，まず，各実験環境の操作に関して，相互に，ある実験環境からすべての実験環境の操作をできるような KVM over IP 装置とリモートログインによる統合操作環境を整備した．実験は，すべてこの統合操作環境を利用して実施した．さらに，各種の設定や制御を統合するために，実験環境の機能を「資源管理機能」と「実験管理機能」の 2 つに大別し，検討を加えた．「資源管理機能」は，各実験環境内の実験ノードなどの資源の割り当てや状態を管理し，「実験管理機能」は，割り当てられた実験ノードへの

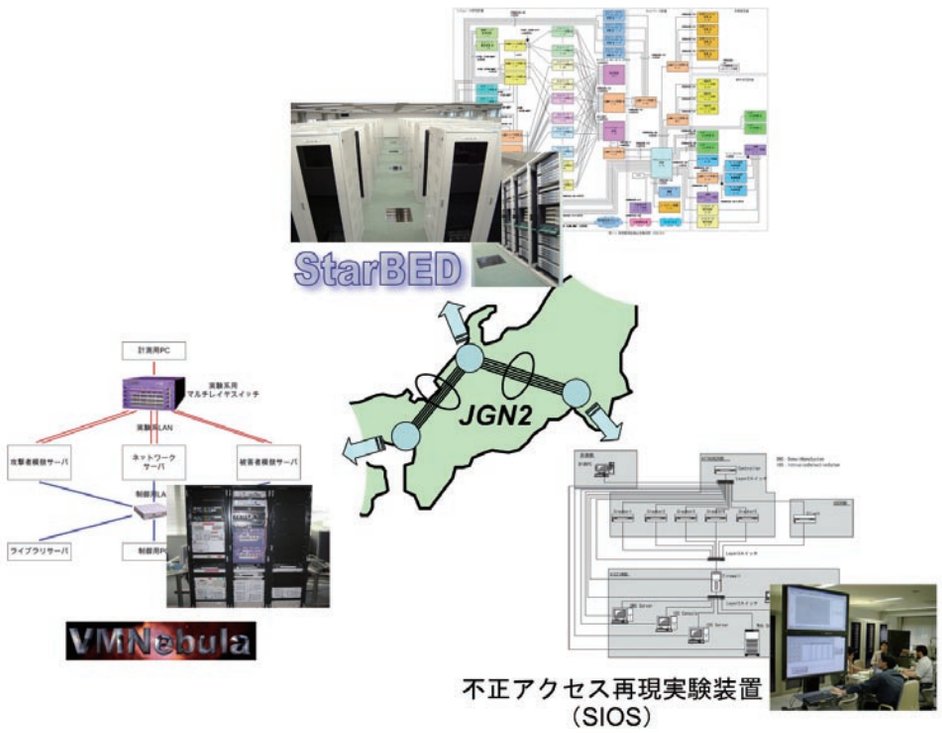

図 -9　3 つの実験環境の連携

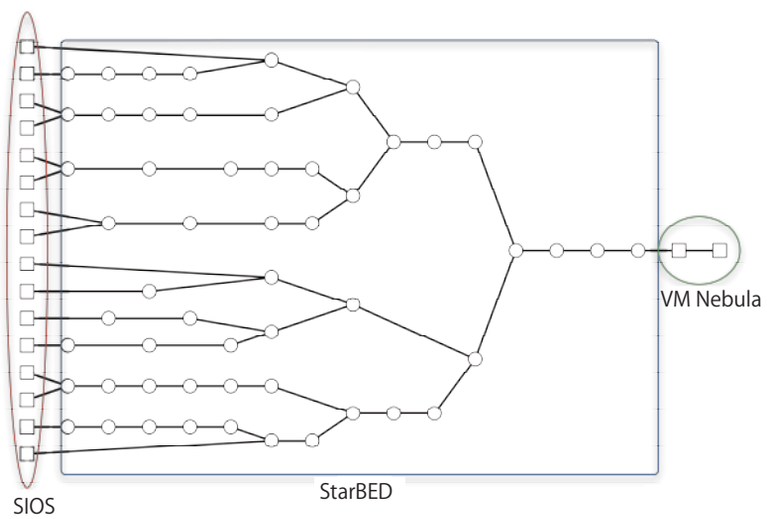

図 -10　模倣実験の構成図

設定の実施や実験の遂行を制御する．それぞれの実験環境にある既存の「資源管理機能」と「実験管理機能」を相互に連携させるための機構を導入することで，統合を図ることができると考えられる．問題は，それぞれの管理機構が持つ機能が統一的でないこと，記述や実現の手法がまったく異なることにある．そこで，「資源管理機能」と「実験管理機能」のそれぞれについて，機能プリミティブ，相互に情報や制御を流通する際のデータ形式とプロトコル，実験環境間インタフェースなどを決定し，複数の実験環境を疎結合させることで統合を図ることとした．

さらに，検討した連携・統合手法について，実証実験により，その効果を確認した．JGN2 で接続された SIOS と VM Nebula，StarBED の 3 つの再現実験環境による連携実験テストベッドを用いて，大規模な攻撃を模倣する実験を行った．内容は，「F5 攻撃（HTTP reload 攻撃）によって対象 Web サーバがサービス不能に陥る」，その後「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」という単純なものである．実験の構成は，図 -10 に示す通り「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 が繰り返し送られる．Attacker ノードから発せられた HTTP request は，StarBED 上の PC ルータを経由

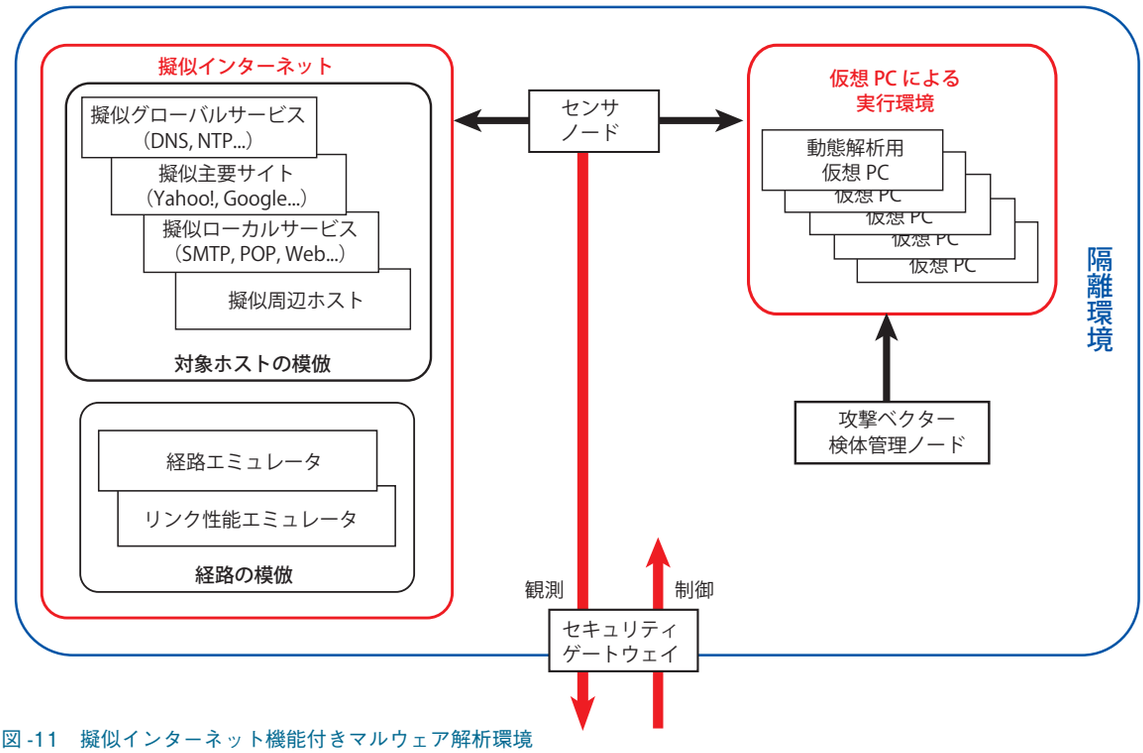

図 -11 擬似インターネット機能付きマルウェア解析環境

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．

上記の実験に加えて，本テーマでは，より実際のインターネットに近い状況を作りだし，実行時に周辺のネットワーク状況を探査し，解析を困難にするようなマルウェアを解析可能とする「擬似インターネット機能」を有するマルウェア解析環境を連携実験テストベッド上に構築した（図 -11）．

破壊的な実験を繰り返し実施する必要があるマルウェアの実行環境として VM Nebula を用い，マルウェアを騙すための擬似インターネットは StarBED 上に構築し，これらを連携させ，解析困難化機能を持つマルウェアの動態解析を試みた．実際に，いくつかのマルウェア検体が，擬似インターネット上に模擬されている偽物の Google などの主要な検索サイトや Microsoft Windows の標準の NTP サーバ time.windows.com などへの到達性を確認することで欺かれ，検査後の動作を露呈させ，解析可能となることを確認した．

ミクロ分析技術の今後

近年，インターネットにおける脅威モデルは急速に進化しており，以前のような脆弱性を突く単純なウイルスの議論では収まらなくなってきている． 本科学技術振興調整費プロジェクト「セキュリティ情報の分析と共有システムの開発」では，新たな脅威モデルに迅速かつ高精度で対応するため，ミクロ分析として不正コードの収集・検知・分析といった一連のプロセス間の連携を強く意識し，それぞれの方式策定から試験評価に至るまで一貫性を持った研究開発を行った．これにより，新たな脅威への耐性を強化することができた．

今後は，個々の分析プロセスの精度，性能，および，連携の向上を図るだけでなく，不正コードに関連する予兆の把握と分析，実ネットワークへの影響度分析など，ネットワークセキュリティ全般に広く関連する研究分野との連携や相互研究が必要になると考える．

参考文献
1) 大平健司，宋 中錫，高倉弘喜，岡部寿男：未知の攻撃コードを安全に収集するための定点観測装置の構築手法，信学技報，Vol.106, No.62, IA2006-1, pp.1-6 (2006).
2) Mori, A., Izumida, T., Sawada, T. and Inoue, T.：A Tool for Analyzing and Detecting Malicious Mobile Code, Proc. of the 28th International Conference on Software Engineering, pp.831-834 (2006).
3) 吉岡克成，井上大介，衛藤将史，中尾康二：感染活動のシミュレーションによるマルウェア影響度分析の提案，電子情報通信学会 情報通信システムセキュリティ研究会 予稿集，ICSS2006-22, pp.67-72 (2007).
4) 三輪信介，宮地利幸，大野浩之：不正アクセス再現実験環境の統合実験，情報処理学会 2005 年マルチメディア，分散，協調とモバイル シンポジウム（DiCoMo2005）論文集，pp.393-396 (2005).

（平成 19 年 6 月 11 日受付）

篠田陽一 shinoda@nict.go.jp
1989 年東京工業大学博士課程修了．北陸先端科学技術大学院大学情報科学センター教授．2006 年（独）情報通信研究機構情報通信セキュリティ研究センター長（兼務）．2007 年 3 月内閣官房情報セキュリティ補佐官（兼務）．ネットワーク分散システム，次世代ネットワークアーキテクチャ，情報環境等の研究を行う．