課題番号１４４

平成２１年度　新規委託研究
マルウェア対策ユーザサポートシステムの研究開発
研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

「マルウェア対策ユーザサポートシステムの研究開発」

２．研究開発の目的

１）背景

近年、マルウェア（不正プログラム）に関して、実行コード（ここではスクリプトまたはプログラムのソースコードを指す。）を意図的に読みにくくする“難読化”や、実行コードが意図的に動的に変更される“自己変貌化”等の手法の開発が進んできている。このような既知のものではないマルウェアに対しては、シグネチャ（マルウェア検査パターン）等の既存技術による検出や駆除だけで対応することには自ずと限界がある。

このようなマルウェアに関しては、感染行動等の挙動を把握することが重要となる。しかしながら、感染しても正規の実行コードを装い、それに気付かせないようにするものや、外部の指令サーバからの攻撃命令を待ち受けるなど、挙動を示すまでに一定の時間を要するものが存在する。このため、ユーザのパソコン内で稼動・常駐しているプログラムがマルウェアであるかどうかを判別するためには、当該プログラムの実行コードを詳細に解析することが現時点で最も有用である。

しかしながら、ユーザのパソコン内で稼動・常駐している多種多様なプログラムのうち、大多数は正規の実行コードであることから、そのようなプログラムの中からマルウェアの疑いのある怪しい実行コードのみを的確に選別することは難しい状況である。

また、ユーザのパソコン上で、実行コードを詳細に解析するにあたっては、処理が重く、パソコンのリソースへの負荷が大きくなることが懸念される。

他方、アンチウイルスソフトを提供するセキュリティベンダーにおいても、このような新しいマルウェアが現出するたびに、詳細な解析を行い、パターンファイルの更新や提供を行ってきているが、ビジネス面の制約などもあり、ユーザが必要なときに、必要なものをタイムリーに提供するところまでには至っていない。

２）目的

上記１）で述べたようなマルウェアに関わる問題に対応していくためには、検出の段階

で、ユーザのパソコン上で不審な挙動がみられるプログラム（正常なプログラムとして登録されていないものなど）を含め、マルウェアに該当する可能性のあるプログラムを、フォールスポジティブ*注1の発想の下で、出来る限り幅広くかつ高精度に検出できるような機能を開発し、検出から取りこぼれるマルウェア（不正プログラム）を最小限にすることが重要である。

また、解析の段階では、当該プログラムがマルウェア（不正プログラム）であるかどうかを正確かつ高速に判別するための高度な解析手法の開発が必要になる。

このような解析機能は、既に、nicter（Network Incident analysis Center for Tactical Emergency Response）*注2において実現されている。nicterでは、ネットワークモニタリングによるスキャン等の振る舞いの把握を目的とする「マクロ解析システム」、収集されたマルウェア（不正プログラム）等の検体の静的・動的解析を目的とする「ミクロ解析システム」、相互の結果を突合し、関連性を導き出すことを目的とする「マクロ－ミクロ相関分析システム」の３つを主要な分析コンポーネントとしており、本研究開発においては、当該解析機能を提供する「ミクロ解析システム」を有効に活用し、効果的に連携していくことが期待されている。

さらに、駆除の段階においては、マルウェア（不正プログラム）の検出・解析と連動して、解析結果に基づいて必要となる駆除ツールを生成し、それを感染に該当するユーザに対して迅速に提供していくための仕組みと必要機能を開発することが重要である。

マルウェア（不正プログラム）の駆除ツールの生成・提供機能については、多種多様なユーザや多種多様なマルウェア（不正プログラム）に対応しなければならない点や、ユーザにとって駆除が必要なときに、タイムリーに駆除ツールが提供されなければならない点等について対応することが重要であることを勘案すると、自動化かつ高速化を図ることが必要となる。

本研究開発は、このような３つの機能を取り込んだ、新たな総合的なセキュリティシステム（以下、マルウェア対策ユーザサポートシステムと呼ぶ。）を構築することを目的として、執り行うものとする。

上記のようなマルウェア対策ユーザサポートシステムが確立されれば、一般ユーザのパソコンの情報セキュリティ向上や一般ユーザへの情報セキュリティ対策の普及浸透につながるだけでなく、一般ユーザにおける情報セキュリティ対策に係るコスト負担の低減や、セキュリティベンダー、サイバークリーンセンター、Telecom-ISAC Japan、

JPCERT コーディネーションセンター等の民間等の取り組みとの連携による当該分野の先導的な研究開発の推進にも直結するなど、大きなメリットを享受できるものと考えられる。

＊注１：フォールスポジティブ　不正でない対象を、“ 不正 ” と誤判定することを許す状態。

＊注２：nicter　情報通信研究機構（NICT）では、広域のネットワークを想定し、スキャンを中心とした攻撃検知とその原因となり得るマルウェア等の解析により、インシデントを迅速かつ正確に検知し、対策を導出するための研究開発を行うために、nicterと呼ばれるインシデント分析センターの構築を進めている。

３．研究開発期間及び予算

研究開発期間：平成２１年度から平成２３年度までの 3 年間

予算：平成２１年度は 237 百万円程度を上限とする。

なお、平成２２年度以降は対前年度比で 6%削減した金額を上限として提案を行うこと。

４．個別研究開発課題

本研究開発においては、以下に示す４つの内容を含む研究開発を行うものとする。

課題ア：検査プログラムに関する研究開発

課題イ：マルウェア駆除ツールの自動生成・最適化・高速検証手法に関する研究開発

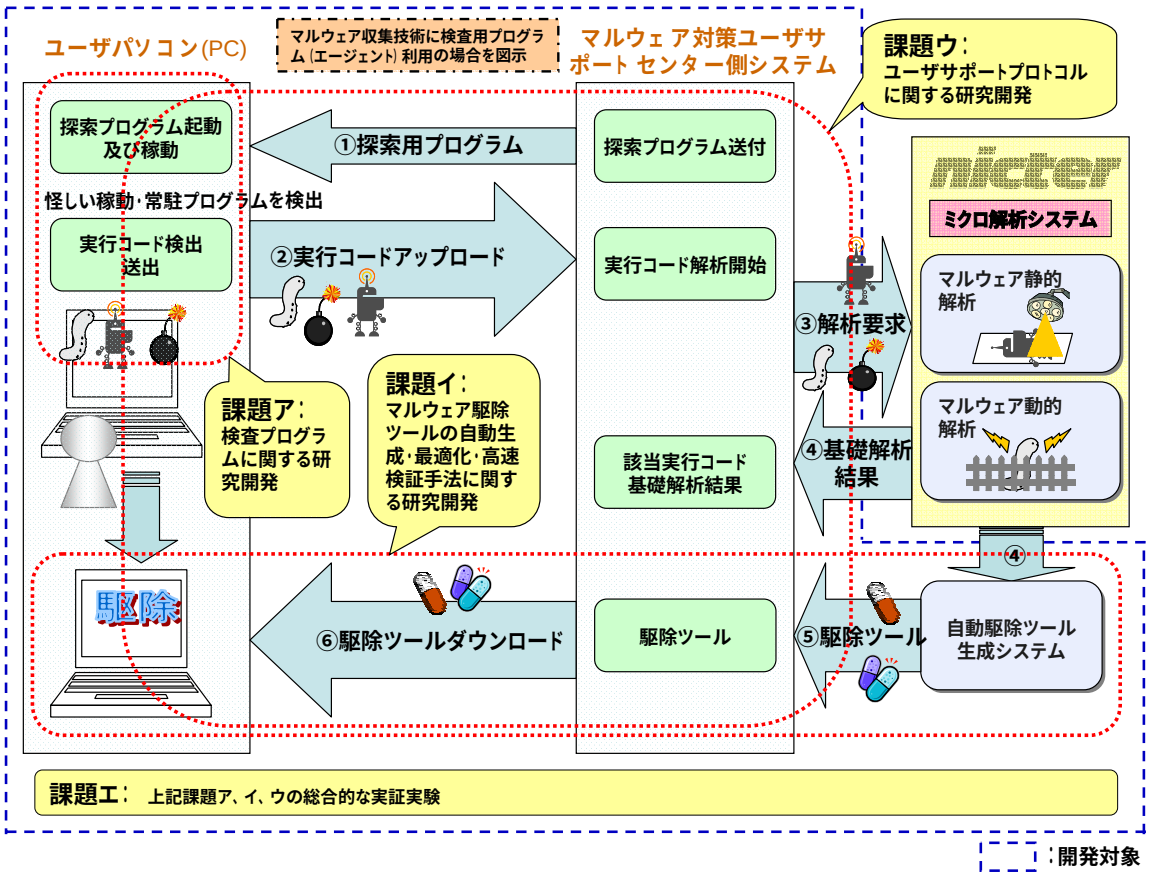
課題ウ：ユーザサポートプロトコルに関する研究開発

課題エ：課題ア～ウを実環境で有効に機能させるための実証実験

本研究開発を実施するに際しては、マルウェアの疑いのある怪しい実行コードの解析を行う部分について、nicter システムを使用し、nicter の「ミクロ解析システム」の機能との連携を図ることを基本とするものとする。

なお、nicter の「ミクロ解析システム」において、マルウェアの疑いのある怪しい実行コードをどの程度適正に解析できるかについては、情報通信研究機構側においても、本研究開発と同時併行で研究開発を進めながら、その実現性の見通しを立てていくことになる。よって、このような解析機能と関わりのある研究開発課題を進めるにあたっては、必要に応じて受託者と情報通信研究機構とが協議して、その進め方や方針について決定するものとする。

本研究開発の全体アーキテクチャ（図１）



さらに、本研究開発では、nicter システムを使用し、nicter の「ミクロ解析システム」の機能との連携を図ることが基本となっている。このため、nicter システムの使用などにつき、以下を考慮する。

①本公募に際し、採択が決定した受託者に対しては、マルウェア駆除ツールの生成等に必要となる実行コードの解析結果を、双方の合意の下で無償で開示することとする。

②また、上記①の際に、どのような形式で実行コードの解析結果を開示するか、どのような方法で実行コードの収集元であるユーザ（パソコン）と実行コードの解析結果を紐付けるかなど、双方の連携が必要となる課題については、情報通信研究機構との協議の上、対応方針や対応方法を決定するものとする。

③nicter システムは、既存機能だけでなく、今後も情報通信研究機構内で継続的な研究開発がなされる。本公募に関わる研究開発の遂行の目的に限定し、nicter システムの使用権を情報通信研究機構が受託者に対して提供することとする。なお、本公募に関わる研究開発で、nicter システムへの組み込みが必要となる部分が発生した場合には、必要な仕様情報などの提供を情報通信研究機構から行うこととするが、機能そのものの組み込みについては、情報通信研究機構にて実施する。

④nicter システムの使用については、上記の合意契約の下、本公募にて示される３年の期間内でその使用が無償で提供される。使用権などに関わる諸権利の整理については、本契約締結後、速やかに実施することとする。

⑤本委託研究終了後に、セキュリティビジネス等を目的として、nicter システムの使用を望む受託者が出た場合には、具体的な連携方策について、別途、受託者と情報通信研究機構が協議を行うものとする。また、受託者が本研究成果を活用してビジネスを展開する際に、nicter システムを使用せず、同機能の実行コードの入手を希望する場合は、適切な対価で実行コードを提供する。

⑥nicter システムに関する問い合わせについては、以下の通りとする。

独立行政法人　情報通信研究機構（NICT）
情報通信セキュリティ研究センター

なお、インシデント分析センターnicter の概要説明については、２０ページ以降の別添資料をご参照ください。

課題ア　検査プログラムに関する研究開発

ユーザのパソコン内で稼動・常駐しているプログラムの中から、マルウェアの疑いのある怪しい実行コードを自動的かつ高能率に探索して収集する、検査プログラムについて研究開発を行う。

課題アー１　不正プログラム基本探索アルゴリズムに関する研究開発

ユーザのパソコン内で稼動・常駐している、マルウェアの疑いのある怪しい実行コードを、フォールスポジティブの発想を採り入れて、ユーザのパソコン上で幅広くかつ高能率に探索し収集する手法の研究開発を行う。

当該探索手法においては、正規の実行コードと、マルウェアの疑いのある怪しい実行コードを効率よく自動識別することが重要となる。

また、コードの難読化や、コードの自己変貌化などの形状変化が見られる実行コードへの対応や、ユーザの多種多様なパソコン利用環境への適応が可能となるよう高精度化を図るものとする。

探索された実行コードについては、適切な形式で複製して収集を図るものとする。

課題アー２　ホワイトリスト化等を用いた高能率探索手法に関する研究開発

課題アー１で賄えない部分を補い、あるいは支援する観点からの取組みとして、正規の実行コードと認識されたものをリスト化（ホワイトリスト化）するなどの手法を用いて、ユーザのパソコンでのリソース負荷を低減し、より高速で高能率な探索手法の研究を行うものとする。なお、必要に応じて、課題アー１との連携を図る。

上記の課題アー１及び課題アー２によって、マルウェアの疑いのある怪しい実行コードを幅広く探索し収集するが、それによってバックエンドの nicter システム（ミクロ解析システム）の処理量・処理時間や、ユーザのパソコンのリソースへの負荷等にどのような影響がもたらされるかについて十分検討するとともに、それらを踏まえて、双方のバランスを十分考慮した適正な探索精度を設定するものとする。

課題イ　マルウェア駆除ツールの自動生成・最適化・高速検証手法の研究開発

nicter システム（ミクロ解析システム）から得られた結果をもとに、ユーザのパソコン利用環境等を踏まえつつ、ユーザがマルウェアを駆除する際に必要となるツ

ールを自動的に生成するための手法について研究開発を行う。

また併せて、生成されたマルウェア駆除ツールの安全性を自動的かつ高速に検証するための手法についても研究開発を行う。

課題イ－１　マルウェア駆除ツールの自動生成・最適化手法の研究開発

マルウェア駆除ツールの自動生成及び最適化を実現するため、ユーザが使用するパソコンの利用環境における各種要素や、パソコンにインストールして実行する際に要求されるマルウェア駆除ツールへの機能的な条件を十分考慮しつつ、マルウェア駆除ツールを構成する必要機能モジュールについて検討を行うとともに、必要機能モジュールを最適な形で組み合わせることにより、自動的にマルウェア駆除ツールを生成する手法の研究開発を行う。

また、生成されたマルウェア駆除ツールに関して、ユーザが使用するパソコンの利用環境（OS やブラウザのバージョン、メモリ容量などのインストール条件や、ネットワーク環境など）に適応できるように最適化するための手法の研究開発を行う。

課題イ－２　マルウェア駆除ツールの安全性の高速検証手法の研究開発

課題イ－１で自動生成されたマルウェア駆除ツールが多種多様なユーザのパソコン利用環境で的確かつ安全に動作するかどうかについて、自動的かつ高速に検証するための手法について研究開発を行う。

当該検証手法においては､マルウェア駆除ツールをユーザのパソコンにインストールして実行したときに、マルウェア駆除ツールが想定した通りの機能やパフォーマンスを達成し正しく実行しているかどうか、マルウェア駆除ツールによる影響でパソコンやパソコン上で動作する他のアプリケーションが正しく実行できなくなることがないかどうか、また、新たな脆弱性につながること、及びマルウェア駆除ツールが悪用されることがないかどうかなどについて、十分検証することが重要となる。

課題ウ　ユーザサポートプロトコルに関する研究開発

クライアントサーバプロトコル、クライアントエージェント、サーバエージェントの３つについて、設計及び開発を行う。

課題ウ－１　クライアントサーバプロトコルの設計及び開発

ユーザのパソコンとセンター側（※）のサーバとの間で、収集された実行コードやマルウェア駆除ツール等を対象として、円滑かつセキュアなデータ伝送を実現するためのクライアントサーバプロトコルについて、設計及び開発を行う。

当該プロトコルの設計においては､クライアント－サーバ間の同期手法や状態遷移管理、エラー処理、秘匿処理について十分考慮するものとする。

（※）「センター」とは、「マルウェア対策ユーザサポートセンター側システム」を指す。

課題ウ－２　クライアントサーバエージェントの設計及び開発

ユーザのパソコン上で､収集された実行コードの送出（センター側のサーバへの送出）に係る指示や、マルウェア駆除ツールのダウンロード要求の着信監視、マルウェア駆除ツールのインストール・実行に係る指示等を的確かつ安全に行うクライアントエージェントについて、設計及び開発を行う。

また併せて、センター側のサーバ上で、受領した実行コードの転送（nicter への転送）に係る指示や、実行コードの解析要求の通知（nicter への通知)、解析結果の着信監視、マルウェア駆除ツールのダウンロード要求の通知（ユーザのパソコンへの通知）等を的確かつ安全に行うサーバエージェントについて、設計及び開発を行う。

また、nicter が提供する「ミクロ解析システム」との連携に必要な機能ついても、研究開発を行う。

さらに､クライアントエージェント及びサーバエージェントに関しては､新たな脆弱性につながること、及びスパイウェアやボット等として悪用されることなど、安全性確保の観点から十分な検証を行うものとする。

課題エ　課題ア～ウを実環境で有効に機能させるための実証実験

課題ア～ウの研究成果と、nicter が提供する「ミクロ解析システム」を統合したプロトタイプシステムを構築し､実証環境において､機能及び性能評価試験を行う。また、ユーザ数による違いや、解析に必要となる実行コードの処理量・処理時間に

よる違い等を考慮して、実証環境にて、上記のプロトタイプシステム上でユーザサポートプロトコルを稼動し、プロトタイプシステムの実用性、スケーラビリティについて評価試験を行う。

５．研究開発課題選定の背景、研究開発の必要性及び他で実施されている類似研究との切り分け、標準化の動向

１）当該研究開発課題を取り巻く現状

ユーザにおけるマルウェア対策として一般的なものは、セキュリティベンダー等が提供している、シグネチャ（マルウェア検査パターン）に基づくアンチウイルスソフトである。アンチウイルスソフトでは、シグネチャを採用しているため、既知のマルウェアに対しては十分対応できるが、未知のマルウェアや、一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードに対しては、現状十分に対応できていない。

また、新しいマルウェアが現出した場合、セキュリティベンダー等が対応するパターンファイルを更新するまでに一定の時間を要するため、ユーザが必要なときに、必要なものをタイムリーに入手できるところまでには至っていない。

その他にも、総務省、経済産業省の連携プロジェクトとして設置されたサイバークリーンセンター（ＣＣＣ）において、ボット対策の一環として、ユーザ向けに、駆除ツール（ＣＣＣクリーナー）が提供されている。このような駆除ツール（ＣＣＣ クリーナー）についても、既に感染行動が見られるボットや既知のボットのみを取り扱っており、アンチウイルスソフトと同様な問題が見受けられる。

また、情報処理推進機構（ＩＰＡ）では、ウイルス情報 iPedia（ウイルス情報データベース）において、届出されたウイルスやボットなどを中心に、それらの主な動作内容や対処法などの解析結果を公開している。

２）研究開発の必要性

コード難読化やコード自己変貌化に代表されるように、昨今、マルウェアの高度化・巧妙化が進展する中で、上記１）で述べた未知のマルウェアや一定期間感染行動等の挙動を見せないマルウェアの疑いのある怪しい実行コードのように、アンチウイルスソフトによる対応では十分カバーし切れない領域が存在している。

セキュリティベンダー等による取り組みを補完しつつ、そのような未知のマルウェア等に

も対応できるように、検体の解析に基づくマルウェア判定をベースとした駆除ツールを、実時間に近い形でユーザに提供していくことが必要になってきている。

３）NICT 及び他で実施されている類似研究との切り分けと、NICT 委託研究における本研究開発課題の位置づけ

本研究開発は、情報通信研究機構（NICT）にて研究開発中の nicter システムを基盤技術として採用することを基本としている。現状の nicter システムにおいては、マルウェアの自動検出・解析技術やマルウェア検体のデータベースを確立することを目的とした研究開発が実施されている。本研究開発は、高度化・巧妙化するマルウェアにも十分対応できるように、マルウェア駆除ツールの自動生成や機能検証等を通じて、このような nicter システムの拡張・高度化を目指すものである。

本研究開発は、個々のユーザのパソコンで検出・収集されたマルウェアの疑いのある怪しい実行コードを、nicter システム（ミクロ解析システム）と連携して解析し、その解析結果に基づきマルウェア駆除ツールを自動生成し、それを個々のユーザのパソコン利用環境への適合性や、安全性を検証しつつ、個々のユーザに提供するものであり、それらの一連のプロセスを実時間に近い形で実現することを目指すものである。

４）標準化の動向

本研究開発のようなマルウェア対策ユーザサポートシステムそのものに関する標準化は行われていない。

６．研究開発の到達目標

全体目標

ユーザのパソコン上で検査プログラムを実行してから、ユーザに対して駆除ツールが提供されるまでの一連の手続きが、１０分程度で完了することを目標とする。

留意点：本研究開発において想定するユーザのパソコンは、Windows OS（XP, Vista）を基本とする。

課題ア　検査プログラムに関する研究開発

課題ア－１　不正プログラム基本探索アルゴリズムに関する研究開発

（１）ユーザのパソコン内で稼動・常駐している実行コード（プログラム）を検査の対象とすること
（２）ユーザのパソコン内で識別された実行コードの中から、不正プログラム（マルウェア）の疑いのある実行コードを抽出するための検出基準を明確化し、導出すること
（３）検出基準の設定においては、未検出の実行コードがないように、フォールスポジティブ的な検出アルゴリズムに基づくこと
（４）上記、検出アルゴリズムは、ユーザのパソコン上で自動稼動すること
（５）対象とする実行コードに難読化や自己変貌化の最新の処理がなされているものに対しても、的確に検出できること
（６）検出性能については、ユーザのパソコンでのコード稼働率やリソースに依存するため、対象とする実行コードのサイズ、種別、数量、及びユーザ環境による検出性能目標を設定し、その評価を行うこと
（７）検出された実行コードについては、サーバへの転送が可能な形式に適切に変換すること

課題ア－２　ホワイトリスト化等を用いた高能率探索手法に関する研究開発

（１）課題ア－１の作業を補足する形で構築することとするが、機能としては疎結合とす

ること

（２）高能率探索（検出）を実現するための具体的な手法を具備すること

（３）既存の正規実行コードリストに加え、サーバ側で実施する解析結果を考慮し、ホワイトリスト手法などを活用すること

（４）高能率探索手法の実現において、インデックス処理などを用いて、ユーザのパソコンでのリソース負荷低減を実現し、CPU 使用率がユーザの体感として支障がないようにすること

課題イ　マルウェア駆除ツールの自動生成・最適化・高速検証手法の研究開発

nicter システム（ミクロ解析システム）から得られた結果をもとに、ユーザのパソコン利用環境等を踏まえつつ、ユーザがマルウェアを駆除する際に必要となるツールを自動的に生成するための手法、及び安全性検証手法の導出を目指す。

課題イ－１　マルウェア駆除ツールの自動生成・最適化手法の研究開発

（１）マルウェア駆除ツールの生成については、nicter システム（ミクロ解析システム）から得られた実行コード解析結果に基づき、自動的に実施すること

（２）ユーザが使用するパソコンの利用環境（Windows OS（XP, Vista）を想定）のそれぞれで実行可能な駆除ツールを生成すること

（３）自己変貌型（ある時間単位で実行コードの形状（ハッシュ値）を変える）の実行コードの駆除のための識別メカニズムを自動導出し、一般的なマルウェアと同等の駆除性能を確保すること

（４）生成されたマルウェア駆除ツールに関して、ユーザが使用するパソコンの利用環境（OS やブラウザのバージョン、メモリ容量などのインストール条件や、ネットワーク環境など）に適応できるように設計すること

課題イ－２　マルウェア駆除ツールの安全性の高速検証手法の研究開発

（１）課題イ－１で自動生成されたマルウェア駆除ツールの検証環境を、想定するユーザの利用環境毎に構築すること

（２）検証環境では、動作の正常性、安全性、効率性の検証が可能であること
（３）駆除ツールの正常性検証においては、通常ユーザのパソコンで稼動している他実行コードとの衝突回避について考慮した上で、衝突が発生した場合には、コードの書き換えなどによって自動生成された駆除ツールの自動再生成を行うこと
（４）駆除ツールの安全性の検証としては、駆除ツール稼動確認テストの自動実行により、不正な実行コードの残存のないことを確認すること
（５）駆除ツールの効率性の検証としては、既存マルウェア駆除ツールと同等の性能を達成すること

課題ウ　ユーザサポートプロトコルに関する研究開発

　クライアントサーバプロトコル、及びクライアントエージェントの設計にあたり、ユーザのパソコンの動作環境を考慮して設計すること。

課題ウ－１　クライアントサーバプロトコルの設計及び開発

（１）クライアントサーバのプロトコル設計にあたり、性能面の最適化、および安全なプロトコル設計を実現すること
（２）当該設計において、適切な状態遷移管理を組み込んだクライアントーサーバ間の同期手法を実現すること
（３）プロトコル設計上で予知できるエラー（状態遷移上）については、適切なエラー処理（たとえば、再送など）の機能を具備すること
（４）当該プロトコルは、ユーザのパソコンで稼動しているセンシティブな実行コード、および対応する駆除ツール（プログラム）を交換するため、適切な暗号化処理、及び鍵管理の機能を具備すること
（５）本プロトコル稼動に伴う、ユーザのパソコンでのリソース負荷を可能な限り削減すること（ユーザの通常プロセスに影響がないこと）

課題ウ－２　クライアントサーバエージェントの設計及び開発

（１）クライアントエージェントは、ユーザのパソコンにおいて軽負荷で安定動作するこ

と

（２）クライアントエージェントは、課題アの探索プログラムモジュール、課題イの駆除プログラムモジュール（ユーザのパソコン上)、及び課題ウー１のプロトコルモジュールを一元的に管理すること

（３）クライアントエージェントにおける管理機能は、実行コードの送出（センター側のサーバへの送出）管理機能、駆除ツールのインストール及び実行管理機能、履歴管理機能、結果報告管理機能などを具備すること

（４）サーバエージェントは、サーバ側に設置するシステムにおいて軽負荷で安定動作すること

（５）サーバエージェントは、課題イの駆除プログラム生成モジュール（サーバ側で稼動)、及び課題ウー１のプロトコルモジュール、及び nicter ミクロ解析システムとの連動管理モジュールを一元的に管理すること

（６）サーバエージェントにおける管理機能は、nicter ミクロ解析システムとの実行コードの要求/応答管理（エラー処理も含む)、駆除ツール生成モジュールとの連携機能、プロトコルモジュールとの連携機能などを具備すること

（７）検証環境では、動作の安全性の検証が可能であること

課題エ　課題ア～ウを実環境で有効に機能させるための実証実験

課題ア～ウの研究成果と、nicter が提供する「ミクロ解析システム」を統合したプロトタイプシステム（評価環境）を構築し、１０００以上のユーザのパソコンを対象として、各課題ア―ウにおいて要求される機能及び性能について実証実験を行うこと。また、ユーザのパソコンが数十万規模になることを想定したスケーラビリティに関する評価検証を実施すること。

７．期待される波及効果

１）類似研究開発面に期待する波及効果

高度化・巧妙化するマルウェアに柔軟に対応可能な新たな総合的なセキュリティシステム（マルウェア対策ユーザサポートシステム）を構築・提供することができるとともに、その中で、マルウェアの疑いのある怪しい実行コードをフォールスポジティブ的に検出できる手法や、超高速に実行コードを解析し、必要な駆除ツールを作成できる手法を確立することができる。これにより、マルウェア対策のさらなる進展への寄与が期待される。

２）実用化面で期待される波及効果

本研究開発の成果については、早期のビジネス上の展開が期待される。このため、受託者の中に、セキュリティビジネスに携わっている事業者、もしくは将来的にセキュリティビジネスに携わる可能性がある事業者が含まれていることがより望ましい。

このようなビジネス上の展開が実現されれば、一般ユーザのパソコンの情報セキュリティ向上や一般ユーザへの情報セキュリティ対策の普及浸透につながるだけでなく、一般ユーザにおける情報セキュリティ対策に係るコスト負担の低減や、我が国の安心・安全なネットワーク環境の実現を後押しする効果が期待される。

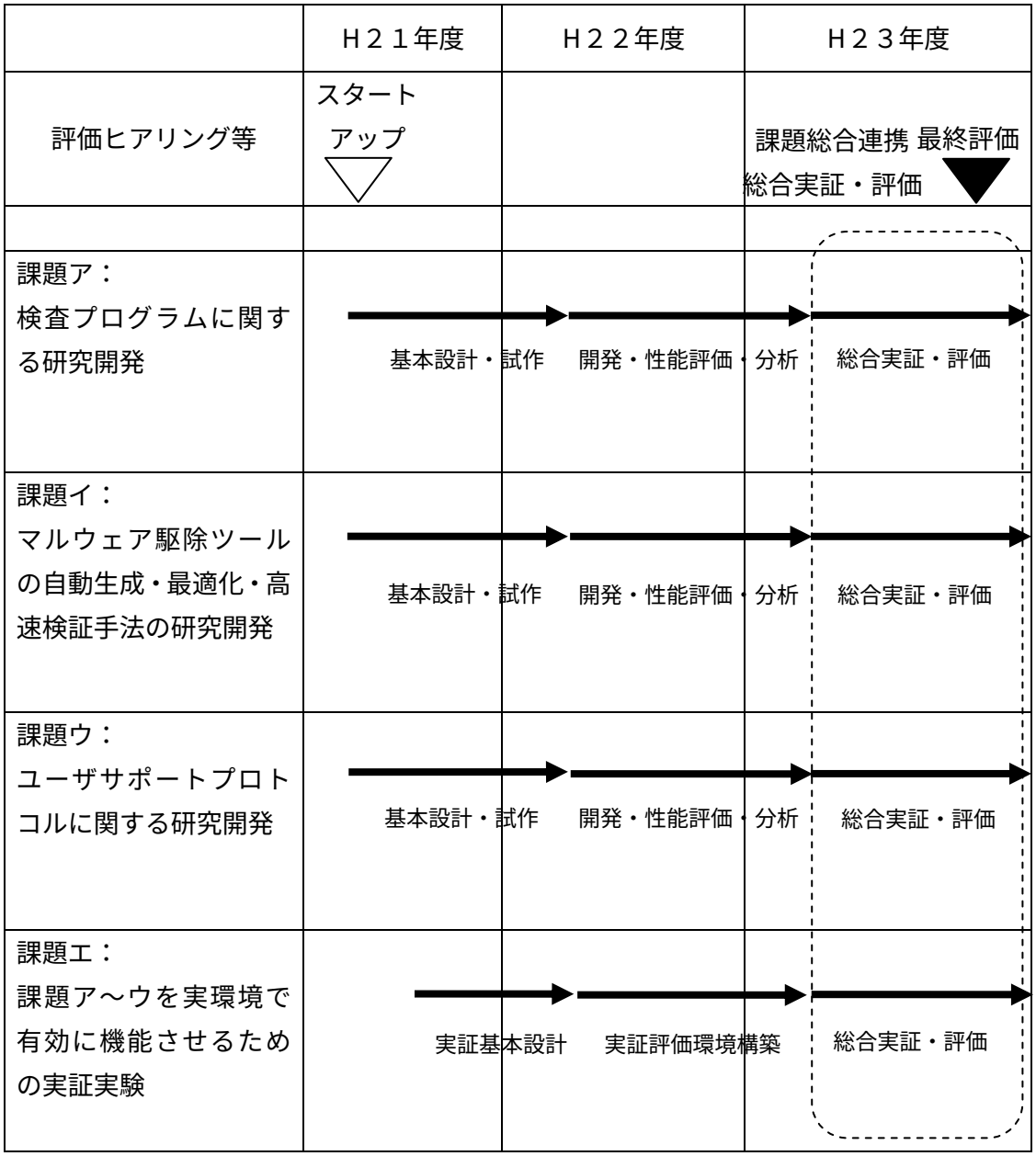
本委託研究終了後に、本研究開発の成果を活用してセキュリティビジネスを展開しようとする受託者が現れた場合に、nicter システムを使用するかどうかについては、受託者の選択に委ねる。

なお、実行コードの解析結果の開示・提供など、nicter システムを使用する場合の具体的な連携方策については、別途、受託者と情報通信研究機構が協議を行うものとする。

３）標準化面で期待される波及効果

本研究開発の成果となる技術は、一般ユーザのパソコンを対象としたマルウェア対策のサポートシステムの運用において、非常に有用な技術であり、ISO、ITU などの標準化団体への提案が想定される。

８．研究開発スケジュール



なお、課題ア～ウの性能評価については、平成２３年度に行う総合実証・評価の前段として、実行コードの種類やユーザ数を小規模に限定した形で、平成２２年度にも評価・検証を行うものとする。

９．研究開発の運営管理及び評価に関する事項

情報通信研究機構は、総務省と密接な関係のもと、プログラムコーディネーター（※１：任命までの間、情報通信セキュリティ研究センター）の助言を受けつつ、本委託研究の適切な運営管理を実施する。外部有識者（評価委員）、プログラムコーディネーター（※１に同じ）の意見を運営管理に適宜反映させるほか、必要に応じて、半年から１年に１回程度本委託研究の進捗状況について報告を受ける等を行う。

最終評価を平成 23 年度に行う。なお、評価の時期については、本委託研究に係る技術動向、政策動向や本委託研究の進捗状況等に応じて、追加の実施、前倒しする等、適宜見直すものとする。

添付資料

インシデント分析センターnicter の概要説明

１．はじめに

nicter は，日本の情報通信基盤の安定運用に資するため，インターネット上で生起する多種多様なイベントの収集・分析を定常的に実施することで，ネットワークに大局的な悪影響を及ぼすインシデントの発生を早期に検出し，迅速かつ実効的な対策導出を可能とする分析センター（かつシステム）の名称である．

nicter は，広域のネットワークモニタリングによって収集したイベントを解析し，その中からインシデントを検出するマクロ解析システムと，マルウェアの検体を収集・解析して，それらの挙動を抽出するミクロ解析システムという 2 つのサブシステム経由の解析パスを持つ（図１参照）．これら 2 つサブシステムにおける解析結果は，相関分析システムにおいてその相関関係が分析され，インシデントの「現象」と「原因」を対応付けることが可能となる．換言すると，マクロ解析システムではネットワーク上で発生しているインシデントの現象を捉えることができ，一方，ミクロ解析システムではインシデントの原因と考えられるマルウェアの挙動を把握できるため，双方の解析結果を照合することで，発生中のインシデントの原因特定が可能となり，さらに，特定されたマルウェアに応じた対策導出も可能となる．その結果，ネットワークモニタリングによって観測された統計データ等の提示に留まらず，インシデントの原因とその対策にまで踏み込んだ実効性・即時性の高いインシデントレポートを，政府・官公庁や一般ユーザに向けて発行できる．

マクロ/ミクロ解析システムならびに相関分析システムの解析結果は nicter の分析者に対してタスクリストとして逐次提示される．分析者はワークフローに沿って各インシデントの候補に対してインシデントの判定を行い，最終的にインシデントレポートの発行を行う．これら分析者による一連の処理はインシデントハンドリングシステム（IHS）と呼ばれる統合的な GUI フレームワークの上で行われる．

以下，nicter のマクロ解析/ミクロ解析/相関分析の 3 つのサブシステムについて概説する．

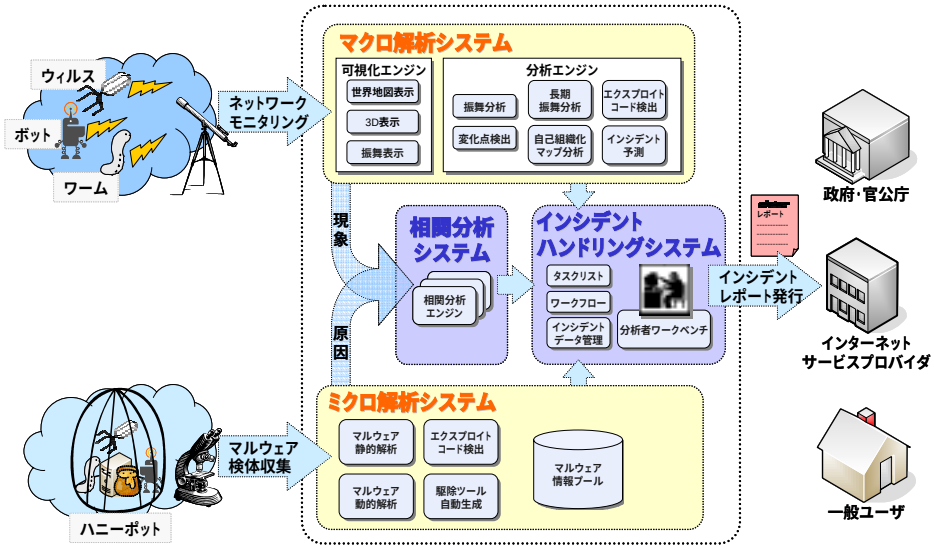
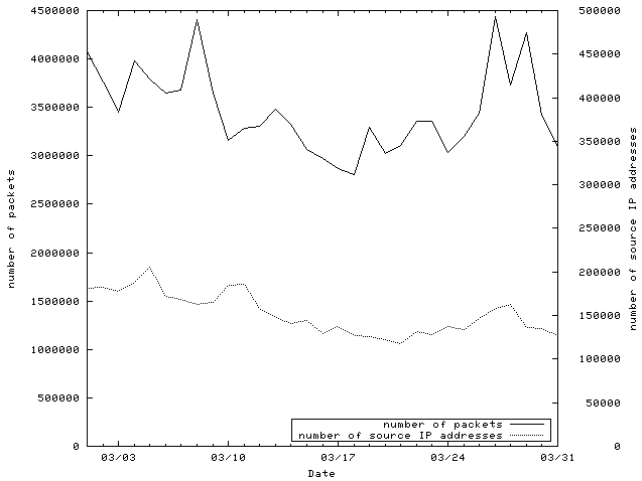


図１：nicter 機能概要図

２．マクロ解析システム

マクロ解析システムは，複数の観測地点におけるネットワークモニタリングで得られたトラフィックを入力として受ける．nicter は現状，日本国内の 12 万を超える未使用 IP アドレスを観測している．未使用 IP アドレスには本来，外部からのパケットは到着しないはずであるが，実際には相当数のパケットが到着する．これらのパケットの多くは，マルウェアの感染行為の第一段階であるスキャンや，DoS 攻撃，送信元 IP アドレスが詐称された DoS 攻撃への返信である Backscatter などが含まれる．図２は nicter の観測対象の/16 ネットワークに 2007 年 3 月に到着したパケット数と，送信元のユニークホスト数である（1 日あたり平均 350 万パケット，15 万ホストからの通信が観測された）．

図２：nicter の/16 ネットワークで観測された



パケット数と送信元ユニークホスト数

このように，未使用 IP アドレスに到着するトラフィックを収集・分析することで，広域ネットワークにおける攻撃活動の傾向を把握することが可能になる．

マクロ解析システムは，分析者による直感的なインシデントの検出を支援する可視化エンジンと，トラフィックの自動分析を行う分析エンジンからなる．以下では，これらエンジンのうちの一部についての概要を述べる．

（1） 可視化エンジン

- 世界地図表示エンジン

ネットワークトラフィックをリアルタイムで可視化する手法の一つとして，nicter では世界地図を用いた可視化を行っている．図 3 は，nicter の観測対象のネットワークに到着したパケットそれぞれについて，送信元 IP アドレスの情報を基に地理的な位置に割り当てて表示したものである．攻撃元からパケットが飛来する様子をリアルタイムにアニメーション表示することで，世界的なマルウェアの活動の動向を直感的に把握することができる．

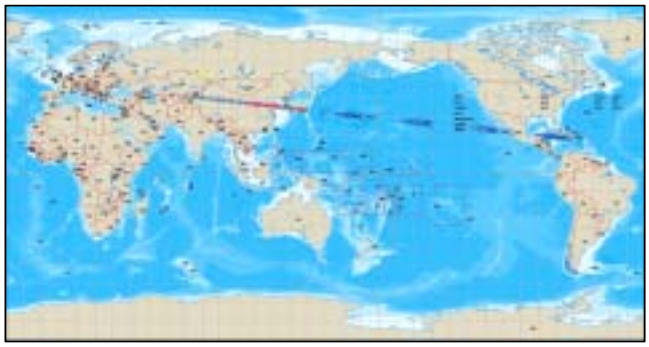


図３：世界地図表示エンジン

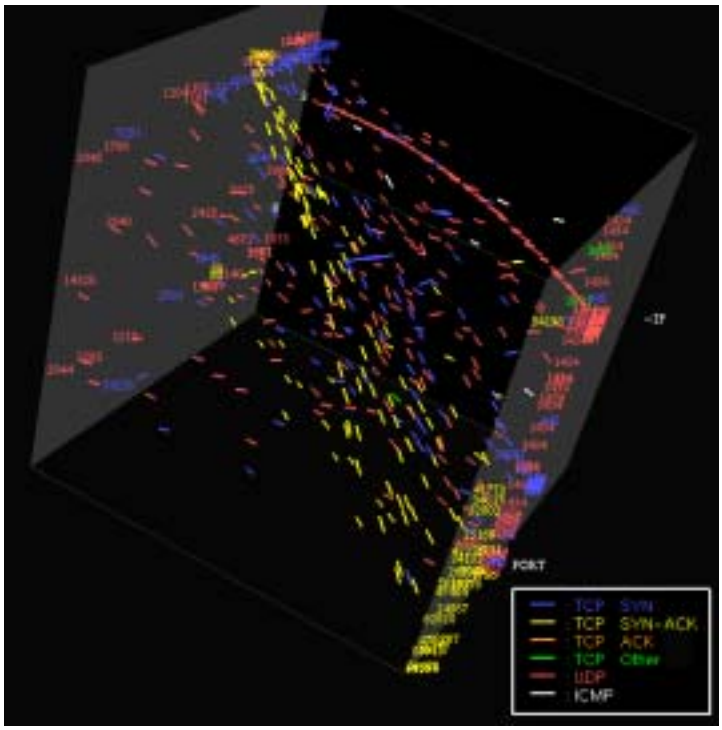


図４：三次元表示エンジン

- 三次元表示エンジン

図 4 は，nicter で観測した各パケットを送信元および宛先の情報（IP アドレス・ポート番号・プロトコル）に基づいて，三次元空間上の立方体中に表示したものである．世界地図表示と同様，リアルタイムにアニメーション表示を行うことで各送信元ホストがどのような攻撃を行っているかを把握することが可能となっている．本エンジンではスキャンの

挙動が特徴的な形状として現れるため，分析者がインシデントの判定や各種の詳細分析を開始するためのトリガを得ることができる．

（2）分析エンジン

- 振舞分析エンジン

振舞分析エンジンは，nicter が観測したトラフィックを送信元ホストごとにスライスし，各ホストの短時間（30 秒間）の振舞を自動分析するエンジンである．以下のパラメータを用いて振舞を自動分類し，DB に逐次蓄積する．

- 送信元/宛先ポート番号
- 宛先 IP アドレス
- プロトコル種別
- スキャンタイプ（Sequential/Random）

この自動分類によって，ある送信元ホストの振舞が既知の攻撃パターンであるのか，あるいは新規の攻撃パターンであるのかを瞬時に判定することが可能となる．

さらに，長期振舞分析エンジンでは，nicter に蓄積された数年に渡るトラフィック情報を長期的なスパンで分析するため，スロースキャン等にも対応可能である．

- 変化点分析エンジン

特定ポートへの単位時間あたりパケット数や，送信元のユニークホスト数などを時系列データと見なし，その急激な変化を迅速に検出するため，nicter では 2 段階の学習アルゴリズムによって高速計算を実現した変化点検出エンジンを用いている．

- 自己組織化マップ分析エンジン

送信元ホストの攻撃パターンの多角的な属性を特徴ベクトルとして自己組織化マップに入力し，同種の挙動を持つ（つまり同種のマルウェアに感染している可能性の高い）ホストをクラスタリングし，クラスタの増減や，発生・消滅などを検出・分析する．これにより，ボットネットの動作の迅速な把握も可能となる．

３．ミクロ解析システム

ミクロ解析システムは，ハニーポット等で捕獲した大量のマルウェアの検体を，1 検体あたり 5～10 分で自動解析し，その性質や挙動を抽出し，マルウェア情報プールに蓄積す

ることを目的とする．以下，ミクロ解析システムの主要なエンジンについての概要を述べる．

（1） 静的解析エンジン

マルウェアの典型的解析法として，マルウェアの実行コードを逆アセンブルして，その特徴を抽出する静的解析がある．しかしながら，マルウェアの実行コードの多くは，逆アセンブルを阻害するコード難読化（code obfuscation）がなされているため，静的解析をより困難なものとしている．そこで，nicter の静的解析エンジンでは，コード難読化されたマルウェアを一旦計算機上で実行し，メモリ上に展開（自己復号）されたコードを取得して逆アセンブルすることで，難読化の効果を無効化可能とする．

（2） 動的解析エンジン

マルウェアのもう 1 つの典型的解析法に，マルウェアを実行状態に置き，その際にマルウェアが使用する API やサーバアクセスなどの挙動を解析する動的解析がある．しかしながら，近年のマルウェアは，自己の周囲のネットワーク環境などを監視して，異常を察知すると沈黙状態となるなど，動的解析を困難にする機能を持つものが多い．そこで，nicter の動的解析エンジンでは，マルウェアを実行する箱庭環境に，DNS や IRC をはじめ多数のダミーサーバを用意することで実インターネット環境を模倣し，スキャンを含むマルウェアの挙動を抽出する．

4．相関分析システム

相関分析システムでは，マクロ解析システムにおいて検出された攻撃パターンを各種の属性に沿ってプロファイル化し，ミクロ解析システムにおいて解析済みであるマルウェアのプロファイルとの照合を行い，インシデントの原因と考えられるマルウェアの候補を探し出す．具体的に，マクロ解析とミクロ解析の相関分析を行った事例を図５に示す．現状の nicter では，類似度がどの程度かを表示することとしており，一番類似度の高いマルウェア（ミクロ解析の結果）から順に表示することとしている．

このように，マクロとミクロの解析結果を照合することで，発生中のインシデントの原因特定が可能となり，さらに，特定されたマルウェアに応じた対策を導き出すことも可能となる．

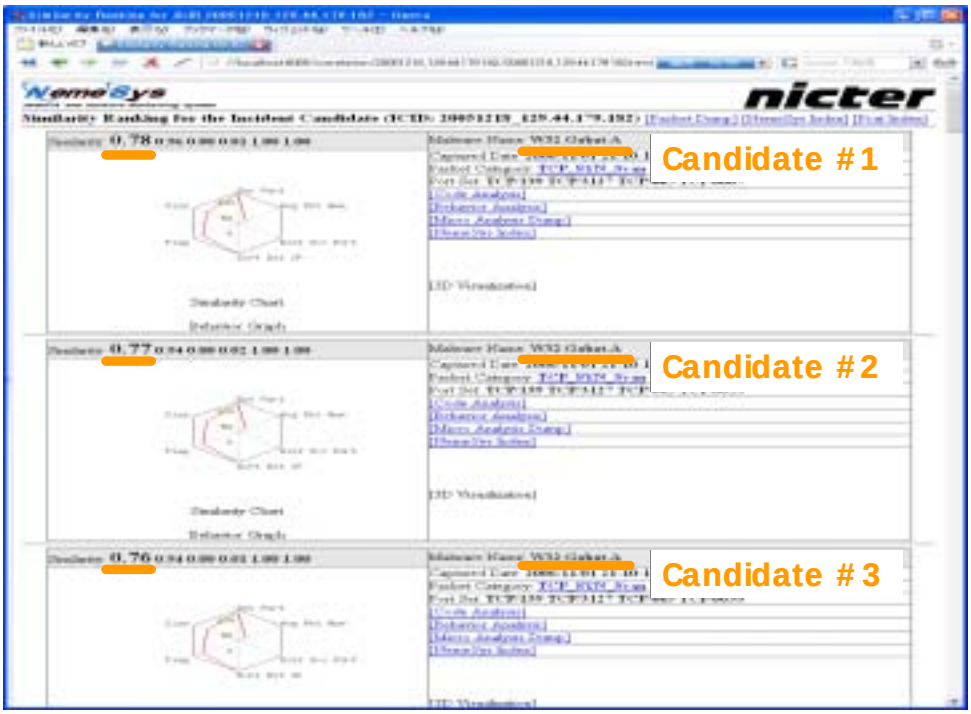


図５：相関分析結果事例

５．今後の研究開発

これまで推進してきた研究開発によって，上述の機能を備えた nicter システムは，一部開発途上部分を残しつつも稼働を開始している．

現状の nicter は，マルウェア解析を機軸とし，マルウェアが放出するスキャンを基礎値とした相関分析に注力している．しかしながら，スキャンはマルウェアの感染行為の初期段階であり，その後にはエクスプロイトコード（計算機の制御を奪うための攻撃コード）の送信，マルウェア本体の感染という段階を踏むことが分かっている．今後の nicter の研究開発では，これまでの研究に加え，エクスプロイトコードやマルウェア本体の感染挙動の段階までの多次元の解析に広げ，より精度の高いインシデント対策を目指していく．