様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ９ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2012～2015
課題番号：２４５０００４３

研究課題名（和文）新しいタイプの攻撃に対するセキュリティ対策を支援する自動トレースの並列分散処理

研究課題名（英文）Parallel and distributed processing of a threat trace for measures for advanced persistent threats

研究代表者

小出　洋（KOIDE, HIROSHI）

九州工業大学・大学院情報工学研究院・准教授

研究者番号：９０３３３５１７

交付決定額（研究期間全体）：（直接経費）　　4,200,000円

研究成果の概要（和文）：本研究の目的は，新しいタイプの攻撃を構成するマルウェアに代表される脅威が，実際的な情報システムに侵入したときにどのような活動が行われるのか，脅威が行う攻撃を阻止したり，情報漏洩を防ぐには何が必要かを明らかにすることである．脅威トレースを実際的な情報システム上で標的型攻撃に使われるマルウェアをシミュレーションするには，並列分散処理による計算時間の短縮化が有効である．そのために，攻撃手法のモデル化と記述方法，タスク並列化に向いた情報システムのモデル化と記述方法，脅威トレースを並列分散化するための技術に関する実装と評価を進めた．またセキュリティ教育に関する適用に関する検討と実装，評価を進めた．

研究成果の概要（英文）：The goal of this study clarify activities of threats. It also clarify that what we need to prevent leakage of secret information, when malware which is used to APT (Advanced Persistent Threat) intrude into practical information systems. Parallel and distributed computation will be effective to reduce elapse time of simulation of behavior of malware on practical information systems. In this study, we make models of attacking methods, models of information systems, notation methods of them. We implement and evaluate them. We also apply the threat tracer to the security training.

研究分野：情報セキュリティ

キーワード：情報セキュリティ　マルウェア　情報システム　標的型攻撃　脅威トレース

１．研究開始当初の背景

1.1 国内外の動向および本研究の位置づけ

近年，企業や政府団体は内部情報網の電子化が急速に進み，現在，企業団体活動に不可欠である製品の設計情報や個人情報等の機密性の高い情報が電子的に管理保管されている．それに伴い，情報システムに対する犯罪行為の目的や手法が変化しており，攻撃者個人が，技術力の誇示，愉快，クレジットカード情報等の個人情報の搾取を目的とした 1 台の PC や Web サーバを対象とした攻撃から，国際的な犯罪組織や国家レベルの機関が企業や組織の気密性の高い情報（例えば，製品の設計情報，知的財産のリポジトリ，メールや文書のアーカイブ，顧客データ）の搾取を目的とした，情報システム全体を対象とした攻撃に変遷してきている．

とりわけ，標的型メール攻撃等に代表される「新しいタイプの攻撃」は，国家のセキュリティや国際グローバル経済活動に関わる特定の組織にターゲットを絞って執拗かつ継続的な攻撃が行われ，攻撃対象の情報システムの特徴や防御策に対応して攻撃手法を変化させ，密かに長い期間をかけた攻撃を行うことが多いとされている．一般には知られてない未発見（ゼロディ）の脆弱性が利用されることも多く，従来のウィルス対策ソフトウェアや侵入検知システムによる対策（入口対策）のみでは不十分で，「新しいタイプの攻撃」を行うマルウェアが情報システム内に侵入し，そこで何らかの活動が行われてしまうことは，完全には防ぎ切れず，企業･組織戦略上重要かつ価値のある機密情報が狙われるという事例も数多く起きている．以下例を挙げる．

・ マイクロソフト社の Internet Explorer に存在したゼロディの脆弱性を利用してグーグル等の米国の特定の企業だけを狙ったオペレーション･オーロラ事件と呼ばれる攻撃が行われ，実際に複数の企業の情報システムが被害を受けた（2010 年 1 月）．

・ Stuxnet と呼ばれる複数のゼロディの脆弱性を利用する高度で複雑な標的型コンピュータウィルスは，特定の国の核プラントという特定のターゲットを狙い，その制御システムに侵入して悪影響を与えるように仕組まれている．そのコンピュータウィルスは 4000 弱の機能を持つ大規模なソフトウェアであり，国家レベルの組織が年単位の期間を掛けて開発したと考えられている（2010 年 4 月）．

・ 東日本大震災の直後から，それに乗じた震災情報の提供を装う標的型攻撃メールによる攻撃が極めて特定の分野の企業に対して集中的に行われた（2011 年 4 月～9 月頃）．また情報収集衛星光学 4 号機の打ち上げ前に開発を行なった企業に標的型メール攻撃が行われた（同年 9 月）．

このように入口対策が困難であるにも関わらず企業団体活動に多大な影響を与える「新しいタイプの脅威」に対する対策，特に機密情報を外部に漏らさない出口対策の必要性が世界的にも高まっている．例えば，内閣官房室セキュリティセンターではリスク要件リファレンスモデルとして調査研究がまとめられ，対策の必要性をアピールしている．独立行政法人情報処理推進機構（IPA）では，新しいタイプの脅威に関連する情報や対策ガイドをまとめて公開し，入口対策だけではなく出口対策が有効であることを説明している．本研究はこの出口対策を支援する有効な情報を提供することを目的としている．

IPA「脅威と対策研究会」は，研究代表者も所属する，情報セキュリティ専門企業，SIer，大学，研究機関などの情報セキュリティの専門家を集めた研究会である．本研究は，この研究会の場を借り，研究に必須となるマルウェアの検体に関する情報，最近の脅威の動向に関する情報，脅威トレースの精度等の評価を中心に，研究会のメンバとの議論や協力を得て実施された．

1.2 過去の研究成果を踏まえて着想に至った経緯

本研究では，新しい分野を開拓する大規模な並列分散プログラムである「 脅威トレーサ」の開発とその並列分散化が主要な課題となる．本研究で提案する脅威トレーサはマルウェアとそれが動作する情報システムを抽象化してモデル化し，その挙動をシミュレーションにより解析する．このシミュレーションの計算時間はノードの個数やマルウェアの複雑さに比例する．大企業や組織の実際的な規模の情報システムに適用したり，数千もの豊富な機能を持つ実際のマルウェアを模擬したりするには多くの計算時間を要するため，並列分散化して高速化する価値は高い．研究代表者は複数のアプリケーションの並列分散化を行った経験があり，それらの研究成果における知見を今回の並列分散化に活かすことが可能である．

また，この部分は情報システムやマルウェアを適切にモデル化し，本研究で設計するDSL（ Domain Specific Language）により表現し，脅威トレーサの一部のデータ構造として適切に組み込まれ実行される．この手法は研究代表者が最も得意とする設計手法にも基づいているものである．またネットワークの各ノードをタスク，ノード間の接続をタスク間の依存関係と考えると，研究代表者が専門とするワークフロー型並列分散プログラム（ タスクが互いに依存関係を持つ並列分散プログラム）のタスクスケジューリング手法を適用可能であると考えられる．

２．研究の目的

本研究の目的は，新しいタイプの攻撃（ APT: Advanced Persistent Threats）を構成するマルウェアに代表される脅威が，実際的な情報システムに侵入したときにどのような活動が行われるのか，脅威が行う攻撃を途中で阻止したり，情報漏洩を防いだりするには何が必要かを明らかにするため，振る舞いパターン等でモデル化された攻撃が情報システム上に加えられたとき，攻撃は情報システム上でどのような経路や振る舞いをとるかを，本研究で提案する「脅威トレーサ」によりシミュレーションする，これにより，実際に情報システム上で何が起きているのかを明らかにし，具体的な攻撃パターンに即したセキュリティ対策を可能化して，現状の脅威に対抗可能な対策や設計に役立つ情報を得ることである．

３．研究の方法

最初に脅威トレースの逐次実装の本研究計画の開始時（2012 年 4 月）まで行った．情報システムとマルウェアの DSL 表現によるモデル化を行った．抽象モデルをステートフルなオブジェクトで表現し，離散イベントシミュレータとして脅威トレースを実装した．次に，本研究期間において脅威トレースを並列分散化するため必要となる要素技術について研究を行った．

具体的な要素技術として，**(1) 攻撃手法のモデル化とその記述方法，(2) タスク並列化に向いた情報システムのモデル化とその記述方法，(3) 脅威トレースを並列分散化するための要素技術に関する検討とその実装をとりあげ，それぞれ，実装と評価を行った．**

さらに脅威トレースがすぐに役に立つことができる応用として，(4) セキュリティ教育に関する適用を検討し，その実装，評価を進めた．

４．研究成果

4.1 攻撃手法のモデル化とその記述方法

本研究の目的は，さまざまな攻撃手法をとる標的型攻撃を脅威トレース上で網羅的かつ自動的に実施することである．標的型攻撃の内容を記述することができる標的型攻撃シナリオを提案し，シミュレーションを自動的に行えるようにした．標的型攻撃シナリオでは，攻撃の段階に一定の独立性があること

に着目し，攻撃段階ごとに攻撃手順を記述できるようにした．この標的型攻撃シナリオに基づいて脅威トレースにシミュレーションを実行させることで，各段階で行われる攻撃における情報システムの問題点を洗い出すことができる．そして，各攻撃段階で明らかになった問題点と「「高度標的型攻撃」対策に向けたシステム設計ガイド」で提案されている標的型攻撃対策のセットを連動させることで効果的な標的型攻撃対策を実現することができる．

提案手法では，情報モデルの選択とモデルに対する操作，操作を実行する順番を定義することで，攻撃手順の記述を可能にした．さらに攻撃段階ごとに個々の攻撃シナリオとすることで，攻撃シナリオの途中で攻撃が成功しなかった場合でも，別段階の攻撃シナリオで情報システム問題点を調査することができるため，網羅性を向上させることができる．また，攻撃段階ごとにシナリオを記述できるため，多くの攻撃手順を記述することなく攻撃シナリオの記述量を削減することができ，シミュレーション時間も攻撃全体を一度にシミュレーションするよりも短くすることができた．標的型攻撃シナリオではシミュレーションの結果と攻撃に対応する対策セットと対応させることができるため，攻撃シナリオでの攻撃の成否から必要な対策を明らかにしやすい．

4.2 タスク並列化に向いた情報システムのモデル化とその記述方法

本研究では，脅威トレースにおける情報システムのモデルの作成と保守を支援することを目的として，システムモデル記述言語に関して設計，実装，評価を行った．

脅威トレースでは，情報システムの情報システムのモデル上でマルウェア等の脅威の振る舞いをシミュレートすることによって，情報システムの設計上の対策の有効性を確認することが可能である．脅威トレースを有効に利用するためには，シミュレーション対象となる情報システムをモデル化して，それを記述できるようにする必要がある．そこで，現在の脅威トレースにおけるモデル記述を，Scala 言語で直接実行できる等の利点は残しつつ，より記述・変更が容易で可読性の高いものにすることより，情報システムモデルの作成と保守を容易する．本研究では，情報システムモデルを扱いに特化したドメイン固有言語（DSL）を実装することでこれを実現した．

結果，構造化された構文や記述の省略を実現することができ，記述・変更が容易で可読性の高いモデル記述となり，情報システムのモデルを扱う際のユーザの負担を軽減することができた．

4.3 脅威トレースの並列分散化

脅威トレースを大規模なネットワークに適用して，実際的な攻撃をシミュレーションすると実行時間を要する．本研究では，その実行時間を短縮化するため，単一の計算機上で動作可能な脅威トレースを分散環境に適用し並列分散実行を可能にする技術を開発した．主に 4.3.1．分散実行機構（旧来の Scala のアクターモデルで実装された脅威トレースのアクターを新しいアクターモデルの実装である Akka を用いた分散実行を可能にするリモートプロシージャコールの実装）と，4.3.2．タスクスケジューリング機構（動的にタスクグラフが変化することに対応できるタスクスケジューリング手法）について検討を行った．

4.3.1．分散実行機構

本研究開始時までの脅威トレースは Scala の Actor フレームワークを使用して実装されていたが，並列分散環境で脅威トレースの実行を行う際，同様にアクターモデルを使用しているが，より新しい実装である Akka を用いると，耐障害性に優れた構築が可能である，スケーラビリティが高い等の多くの利点が

得られる．そこで脅威トレースを，Akka を用いて，分散環境で実行することを検討した．この際にアクターに定義されたメソッドを直接呼び出している部分を，Akka の純粋なアクターモデルに対応するために，Method Missing による送信処理，および Reflection による受信処理により，リモートプロシージャコール（RPC）を実現し，呼び出せるようにした．実際に分散環境上で想定通りに動作することを確認した．これにより脅威トレースだけではなく，旧来の Scala のアクターモデルで記述された Scala のプログラム全般を新しい実装である Akka 上にポーティングすることが容易にすることもできた．

4.3.2. タスクスケジューリング機構

実際の攻撃を模擬する脅威トレースは，攻撃に使うマルウェアが生成消滅したり，情報システムの構成が変化したりすることで，実行後にタスクが追加・分割される動的なアプリケーションである．この種のアプリケーションは特殊なものではなく，例えば Web アプリケーションにおいても外部からの作用により，後からタスクが生成・消滅する．このようなアプリケーションを効率良く実行するためいは，実行単位となる各タスクをタスク間の依存関係に基づき，どのように各計算機に割り当てるかというタスクスケジューリングが課題となる．現在までにタスク間の依存関係や計算機，ネットワークの負荷状態を考慮して全体の計算時間を短くするタスクスケジューリング手法が多く提案されている．しかし，動的にタスクが生成・消滅することにより，タスクグラフが変化することに対応できるタスクスケジューリング手法は提案されていない．そこで，著者らが提案したスケジューリング手法の 1 つである CP/ETF/MISF 法を基本に，タスクグラフの動的な変更に対応できる新しいタスクスケジューリング手法を提案し評価を行った．これにより動的にタスクグラフが変化するアプリケーションにおいても効率的に実行できることが分かった．

4.4 脅威トレースの攻防戦化

本研究の目的は，情報システムの設計者や管理者が攻撃者側の視点を得ることを支援することにある．近年のサイバー攻撃は高度に洗練されており，IDS やファイアウォール等の従来の対策では防ぐことが困難である．特に，情報システムを入念に調査された複雑な標的型攻撃，APT(Advanced Persistent Threats)攻撃と呼ばれるタイプの攻撃に対して防御するには，情報システムそのものに関する知識を向上することに加え，攻撃者からの視点を得ることが特に重要となる．この種の攻撃は，段階を踏んで計画的に行われることが多い．そこで本研究では，脅威トレースがすぐに役に立つことができる応用として， 攻防戦演習に応用することにより，情報システムの設計者や管理者が攻撃者側の視点を得ることを支援することにより，情報セキュリティ技術の向上を支援することが可能となるようにした．具体的には，実際の標的型攻撃の事例やマルウェアの動作を元にした攻防戦のシナリオを攻撃側と防御側で実現できることを確認することができた．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

1. 加藤雅彦, **小出　洋**, 金岡　晃, 松川博英, 前田典彦，岡本栄司：*HTTP プロキシサーバでの Cookie 挿入によるバックドア通信の検出*, 情報処理学会論文誌, *Vol. 55, No. 9, pp.2008-2010 (2014)*（査読有）.
2. 甲斐夏季, **小出　洋**：*LSI 論理シミュレーションにおける SIMD 並列化手法の提案*, 情報処理学会論文誌 コンピューティングシステム，*Vol. 7, No.1, pp. 46-56 (Mar. 2014)*（査読有）.

〔学会発表〕（計 10 件）

1. 神武克海，小出 洋：脅威トレースの攻防戦化，情報処理学会九州支部火の国シンポジウム2016（2016年3月2日-3日，宮崎市）.
2. 熊野修平，Dirceu Cavendish，小出 洋：分散 XML 処理のためのルーティングアルゴリズムの提案，情報処理学会 第 107 回プログラミング研究会(2016 年 1 月 13 日-14 日，福岡市）.
3. 三牧麻美，小出 洋：動的なアプリケーションに対するスケジューリング手法の提案，情報処理学会 第107回プログラミング研究会（2016年1月13日-14日，福岡市）.
4. 松元拓也，三牧麻美，神武克海，小出洋：脅威トレースの並列分散化，情報処理学会第56回 プログラミングシンポジウム予稿集，pp.151-159 (2015年1月9日-11日，伊東市).
5. 山口凌，熊野修平，村上隆俊，小出洋：脅威トレースのためのシステムモデル記述言語の実装，情報処理学会 第56回 プログラミングシンポジウム予稿集，pp.33-45 (2015年1月9日-10日，伊東市).
6. Murakami, T., Kumano, S. and **Koide, H.**: An Implementation of Tracing Attacks on Advanced Persistent Threats by Using Actors Model, In Proc. SCIS (December 3-4, 2014, Kitakyushu, Japan)（査読有）.
7. 田坂祐太，小出 洋，乃万 司：トランスポート層におけるインテグレーテッドマルチVPNの提案と遠隔医療への適用，電子情報通信学会技術研究報告，Vol. 114, No. 139, IN2014-45, pp. 89-94 (2014年7月10日，札幌市).
8. Kato, M., Matsunami, T. Kanaoka, A., **Koide, H.** and Okamoto, E. : Tracing Attacks on Advanced Persistent Threat in Networked Systems, In Proc. SafeConfig 2012 5th Symposium on Configuration Analytics and Automation (October 3-4. 2012, Baltimore, MD, USA)（査読有）.
9. Kai, N., Nishinohara, R., **Koide, H.:** A SIMD Parallelization Method for an Application for LSI Logic Simulation, In Proc. SRMPDS, ICPP Workshops, 2012, pp. 375-381 (September 10-12, 2012, Pittsburgh, PA, USA)（査読有）.
10. Uratani, Y., **Koide, H.,** Cavendish, D. and Oie, Y.:Distributed XML Processing Over Various Topologies – Pipeline and Parallel Processing Characterization, In Proc. WEBIST 2012, pp. 116-122 (April 18-21, 2012, Porto, Portugal)（査読有）.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕

６．研究組織
(1)研究代表者
小出　洋（KOIDE HIROSHI）
九州工業大学・大学院情報工学研究院・准教授
研究者番号：90333517