様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２６ 日現在

機関番号：３２７２１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９７４

研究課題名（和文）高信頼アクセス制御をベースとする知的侵入検出・防御方式

研究課題名（英文）Intelligent Intrusion Detection and Protection Method Based on Reliable Access Control

研究代表者
橋本　正樹（Hashimoto, Masaki）

情報セキュリティ大学院大学・その他の研究科・准教授

研究者番号：１０５８２１５８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：本研究は、知的侵入防御システムとして、コンピュータ内部の悪性活動を従来方法以上の高い精度で検出した上で、その動作を的確に抑制する方法を設計・実装し、その有効性を検証することを目的とするものである。本研究は3年間で実施され、主な研究成果は、システム内部の悪性活動の紐付け手法と可視化に関する検討・実装・評価を行い、提案手法が実際に行われた攻撃シナリオをシステム内部の悪性活動として過不足なく捕捉できることを実証したことと、その結果、セキュリティ・エンジニアが、従来の手法と比した時に容易に悪性活動の発見・対処を行うことができることを実験により確認したことにある。

研究成果の学術的意義や社会的意義
侵入検知・防御システムのアプローチを整理すると Misuse(Signature)-based Detection と Anomaly Detection の二つに大別できる。近年の高度標的型攻撃に対して前者はほぼ無力であるため、後者を主に対処を図るケースが年々増加しているが、そもそもが機械学習や統計的処理に利用可能なデータに乏しいことに加えて、人間の専門的知識や経験に頼る部分が大きく、人的負荷が非常に高い。本研究は、機械学習等による相関関係ではなく、推論による因果関係の分析による悪性活動の検出と対処により、既存の様々な研究とは異なる方向性からの上記課題解決を志向したことに学術的意義がある。

研究成果の概要（英文）：The objective of this research is to design and implement a method to detect malicious activities inside computers with a higher accuracy than conventional methods and then precisely suppress such activities as an intelligent intrusion prevention system, and to verify the effectiveness of this method. The main results of this research, which was conducted over a three-year period, were the study, implementation, and evaluation of methods for linking and visualizing malicious activities inside the system, and the demonstration that the proposed method can capture actual attack scenarios as malicious activities inside the system without excess or deficiency, and the result of the study that security engineers The experiments confirmed that the proposed method can detect and deal with malicious activities more easily than the conventional methods.

研究分野：情報セキュリティ

キーワード：侵入検知・防御　オペレーティングシステム・セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景
情報システムへの悪意ある攻撃は、現代社会に大きな脅威となっている。サイバー攻撃の高度化に伴って、侵入や攻撃を未然に抑制することは困難になりつつあり、防御法は、侵入を受けても早期に侵入を検出・特定し、被害を局所化し、排除する技術に移りつつある。ここでの学術的課題は、情報システムの中で起こっているファイルやネットワークへのアクセスが許可された正当な動作であるか､侵入者による悪性活動であるかを判別する方法である｡判別が可能になれば、不正な動作をアラートするだけでなく、セキュア OS 等のアクセス制御システムによって、攻撃を止めることが可能になる。

悪性活動の検出と防御には、オフライン型の手法として、(1)悪性活動を行うマルウェアを事前に収集・解析し、その特徴との類似性から未知攻撃の検出を目指すもの、(2)システムの各モジュールが生成するログを集積し、その中のセキュリティ関係イベント間の統計的な相関分析を行い、怪しいものの検出を目指すものがある。相関分析には、ニューラルネットワーク等の機械学習によって相関学習を行う試みがある。オンライン型の手法としては、(3) システムに到着するデータの中に既知のマルウェアの痕跡を探すシグナチャ手法、(4)プロセスがアクセスして良い資源､禁止する資源をあらかじめ登録し､OS がアクセスを監視するセキュア OS などがある。

これらに共通するのは、悪性活動の検出に先立って、悪性活動とは何であるかを悪性活動の前例から抽出しておくことである。オンライン型の手法は、リアルタイムで判別しているように見えるが、シグナチャの作成にはマルウェアの検体が必要であるし、セキュア OS は、通常状態で長期間運用することで通常状態でアクセスして良い資源のリストを作成する必要がある。すなわち、ほとんどの悪性活動検出法が、悪性活動の証拠を見つけた後にその悪性活動を排除する戦略を取っているので、セキュリティ対策は常に後手、後手に回り、ゼロディ攻撃に晒され、常に攻撃者優位と評される関係が変わらない。

そこで、悪性活動の検出・防御に関する学術的問いは、未知の悪性活動を検出し、排除することができるかということになる。さらにこの問いを詳細化すると、i) 悪性活動（の元となるマルウェア）を個別に、すべて知っておく必要があるか、ii) 個別活動の一連の集合として発現する悪性活動を事前に定義し、これに基づいた防御が可能であるか、ということに帰着する。

しかしながら、i については、個別マルウェアの詳細な分析が必要であるが、近年はマルウェア種は数億に上り、それぞれは難読化を施されているため分析や判別が困難になっている。また、ii については、システム全体をログ履歴をあらかじめ収集して相関分析を実施する必要があり、悪性活動の例を多く集めるまで、正確な判別を期待できない。また、異常を発見して直ちにその動作を抑制・停止させるリアルタイムの制御が難しい。 一方で、セキュア OS では、重要なファイルやネットワークホストへのアクセスを検出して、悪性活動を識別しようとするが、個別のアクセスだけで識別するので、正常な行為を悪性と識別する可能性もあり、また誤認識を恐れて設定を緩くすると悪性活動を見逃すというジレンマがある。

これらからわかることは、個別の行為だけに注目して判別をするのは不十分であり、統計的な情報に頼る方法では、悪性活動の事例を多く必要とするということである。したがって、悪性活動の事例を収集することなく、より大局的な情報に基づいて、正確な侵入やマルウェアの悪性活動を検出して止めることができるかどうかが、学術的な問いとなる。また、工学的には、この手法がシステム本来の活動に実行効率等において悪影響を与えないか、悪性活動パターンがルールとして適切に記述できるか、実システムに円滑に適用できるかなどの疑問に答える必要がある。

２．研究の目的
本研究では、知的侵入防御システムとして、コンピュータ上の悪性活動を従来法以上の高い精度で検出し、その動作を的確に抑制する方法を設計・実装し、その有効性を検証することを目的とする。提案手法において、オペレーティングシステムが、システム内プロセスのファイルアクセス、ネットワークの送受信、プロセスの起動、権限の変更などの要素動作の実行列を観測する方法を研究する。システムの設計者・運用者は、想定される悪性活動をこれらの要素動作の連関パターン（プロセス活動ネットワーク PAN: Process Activity Network）として記述するが、それに適した専用の言語を設計する。この言語では、特定の活動パターンが持つ活動意図をルールに則って推論し、悪意活動の自動判定と適応対処を記述する。OS としては、セキュア OS として実績のある TOMOYO Linux を用い、TOMOYO Linux の LSM（Linux Security Module）として、この専用言語を解釈実行して悪性活動を検出・抑制する機能を付加する。

従来法としては、大量のマルウェアの分析から特徴的な悪性活動を抽出する方法、SIEM が行うような、プロセスの実行ログの統計的分析から悪性活動の兆候を確率的に推測する方法、正常なプロセス活動の履歴から異常活動を検出するセキュア OS などがある。これらに比して、提案手法は、推測される悪性活動を事前にルールとして記述し、セキュア OS にそのルールの実行系を搭載し、OS が観測する実行プロファイルを入力として、悪性活動をルールベースで推定するという違いがある。ルールに基づいて悪性活動を推測するシステムは例がなく、本研究の新規な提案となる。要素活動の順序や組み合わせから判別を行うので、「パスワードファイルへのアクセスは悪性活動としてすべて禁止」のような大ざっぱな判別法に比して、悪性活動を限定的に判別可能であり、従って、通常のオペレーションに支障が生じる事態を回避しやすい。また本提案は、セキュア OS に組み込むので、悪性活動が検出されるとただちに当該活動を抑制・停止させられるという効果もある。その代償として、セキュア OS がシステムサービスを行うたびにその活動を記録し、悪性 PAN ではないかを判別するオーバヘッドが加わる。したがって、パターンマッチをキャッシュするなどしてこのオーバヘッドをどこまで減じられるかも重要な課題となる。

３．研究の方法

研究代表者らはこれまでの研究[1、2]において、細粒度アクセス主体の同定手法と、高レベルアクセス判定手法を提案した。細粒度アクセス主体同定は、アクセス主体プロセスの出自や、生成プロセス系列・SVC リスト他の処理履歴を抽出して実現し、高レベルアクセス判定手法は、仕様レベル記述による簡潔なポリシー表現を可能とする言語により実現している。また、これら要素を、研究協力者がプロジェクトリーダを務める TOMOYO Linux 上で実験的に実装し、その性能評価等を実施済みである[3]。TOMOYO Linux は、バージョン 2.6.30 以降の Linux カーネルに組み込まれ、OSS として開発が続けられている国産のセキュア OS モジュールである。

本応募課題では、これらの成果を基に開発済みの要素を結合して高信頼アクセス制御機構のプロトタイプを実装し、研究の基盤とする。その上に、システム内活動の紐付けを実現し、その意図解析による侵入検出機能を実装して、知的侵入防御システム（図 1）を実現する。更にそれを評価して、この提案の有効性を示す。すなわち、３年内で以下の研究を行う。

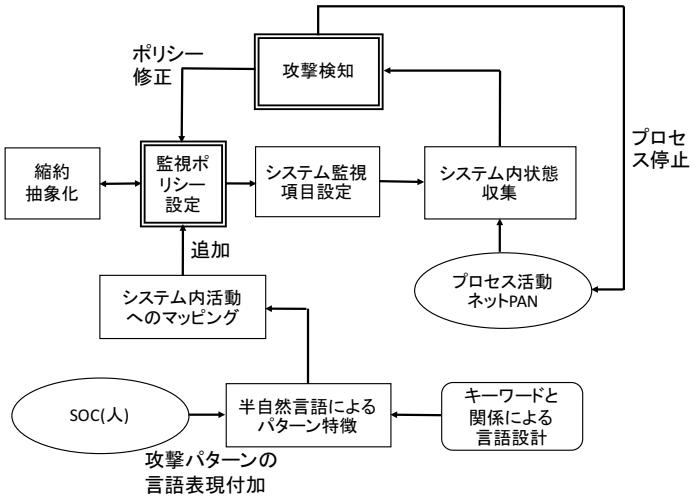

図 1 適応型知的侵入防御システム

1. これまでの研究で明らかにした、細粒度アクセス主体同定手法と、論理型言語による高レベルのアクセス判定手法を実装した高信頼アクセス制御機構のプロトタイプを実現する。また、分散系への拡張についても、授受プロトコルを設定することで実装する。
2. 様々なシステム内プロセス活動をその生成源同定によって互いに紐付けし、PAN に活動パターンとして蓄積する方式を実装する。例えば、メール受信・実行コード挿入・ファイルアクセス・メール送信トライ、といった一連の攻撃をプロセス生成とその結果という関係を用いて紐付け蓄積し、新たな活動が生成されると、それとの紐付けをチェックしてその蓄積を更新する。
3. PAN から意図を抽出する手法を開発する。ここで言う意図とは、例えば、「外部指示で重要情報の送出」といったもので、2 の例では、メール送信先から「外部」を、ファイルのメタ情報から「重要情報」を、メール送信から「送出」を推論し、意図の成立を見出す。また、検出した侵入への対応として、関連する活動パターンを対象に送信停止や状況レポートを作成する。
4. 侵入の検出結果を集積し、攻撃意図の収集からその変化を調べ、縮退させた形で新たに設定するべき「新意図」候補の抽出を行う。それを検出ターゲットに設定することで、変化への適応能力を持たせるとともに、結果を管理者に提示する。

5. 提案システムを実際の様々な侵入攻撃例に適用し評価する。

提案システムを実現するポイントは、様々なシステム内活動を洩れなく、原因–結果のリンクで接続する所にある。それは、メール等の添付実行コードを実行したとき、それから生成されるすべての活動をそれに紐付けることを含んでいる。従って、提案方式は、相関分析とは異なり、活動パターンそれぞれ内の活動要素には確実な関係が存在し、結果として、論理的に活動パターン内悪意の存在を検出可能で、管理者が指定する「検出すべき意図」を持つ侵入を確実に把握できる。これは一般に複雑な作業であるが、テイント解析の手法をベースに実現する計画である。

４．研究成果

2019 年度の研究では、システム内悪性活動の紐付け手法と可視化を検討した。検討には Linux において監査ログを取得する Audit フレームワークより、特定のシステムコールの情報を用いた。侵入検知手法に関しては既存の環境にある IDS/IPS による検知をトリガーとし、特定ホストの悪性活動の紐付けを行う想定で行った。紐付けにはプロセスの親子関係、ファイルとの関係を用いることで、必要な範囲のログを収集した。いくつかの攻撃シナリオを再現した結果、攻撃活動の分析に必要な情報の紐付け、可視化が可能であることを確認した。特にファイルとの関係を用いた紐付けにより、通常は関連付けることに手間がかかる、親子関係の無いプロセス同士を結び付け、1 つの活動として分析するにあたって必要な情報として取得できることを示した。本研究で提示したプロトタイプを SOC の監視員が活用することで、IDS/IPS の情報に加え、より詳細なシステム内の活動を特別な作業を行わずに分析することが可能になると考えられる。特にネットワークのログだけを監視している環境において誤検知が頻繁に発生する状況であっても、本当に対応が必要な分析につながると考えられる。また、インシデント発生時の攻撃活動調査をする際にはシステムを停止し、OS に精通した技術者による調査を行うことがある。プロトタイプで利用しているシステムコールは得られる情報の粒度が細かく、全てのシステム内活動を漏れなく取得し、それらをリアルタイムで解析可能な仕組みとなっているため、予め詳細に調査する必要のあるプロセス、ファイルを一覧化できる等、攻撃調査を簡略化することにも繋がると考えられる。

2020 年度の研究では、第 2 ステップまでで開発したシステムの評価方法を検討すると共に、第 3 ステップに関するプロトタイプ設計を行なった。すなわち、第 2 ステップまでの評価方法としては、開発した紐付け手法が、様々なシステム内活動を人間が識別して理解し、ルール記述が可能な粒度での自動的な紐付けができているか否かに焦点をあてる評価方法を設計し、人間を対象とした評価実験を実施するための追加の開発を行なった。具体的には、システム内活動ログの収集・格納・検索を各々Auditbeat、Logstash、Elasticsearch 等の OSS を利用して実装し、それらを Python で記述したプログラムによって統合・分析するシステムを構築した。また、この結果を人間に提示する視覚化部分については、Cytoscape、KIBANA を用いて実装した。このシステムを用いた具体的な評価実験としては、研究代表者の研究室構成員を中心としたセキュリティエンジニアを対象に、IDS が不審な通信を検知し、その IP アドレスからその原因となっているプロセスを特定するシナリオを想定した上で、複数評価指標に関するアンケート調査を行い、その結果を分析した。また、第 3 ステップのプロトタイプ設計としては、構成した PAN に混在する通常活動と悪性活動について、それらを識別するためのルールの記述方法と、記述したルールから意図を抽出する手法に関する検討を行った。2019 年度までの研究成果については、2020 年度に国内の関連シンポジウムや研究会等で発表済みであり、2020 年度の研究成果の発表については、関連国際会議と論文誌にて発表するための準備が済んでおり、近日中に投稿予定である。

2021 年度の研究では、2020 年度までに検討した手法をシステムとして実装し、その評価と外部発表を行った。開発したシステムは、これまでの検討内容を実際の Linux システム上に実装したもので、IDS/IPS 等で外部との不正な通信を検知した際に、その攻撃源を見つけるシナリオを想定し、システムコールログを半自動的に解析した上で、関連するプロセス及びファイルを一連の悪性活動として紐付け･可視化することを実現したものである。このシステムの評価としては、i) 具体的な攻撃シナリオを再現し、悪性活動の紐付け・可視化ができることの確認、ii) i)の紐付け・可視化が人間による分析の支援となることの確認、iii) 様々な現実の攻撃シナリオで悪性活動の紐付け・可視化ができることの確認、を行い、この有効性を示した。
また、このシステムの開発によって明らかになった課題、すなわち、一連の悪性活動を紐付ける際の、依存関係の爆発問題への対処方法、必要十分な分析期間の設定方法、時系列情報の表現方法、紐付け及び可視化の完全自動化方法、分析支援効果についてのより適切な評価方法等については、引き続き検討を進めた。同時に、このシステムをベースに、侵入の検出結果を集積し、攻撃意図の収集からその変化を調べ、縮退させた形で新たに設定するべき「新意図」候補の抽出を行う手法の検討と、それを検出ターゲットに設定することで、変化への適応能力を持たせるとともに、結果を管理者に提示する手法についての検討を行った。

〈参考文献〉

1. “論理プログラミングを基礎とした認可ポリシー記述言語”、 M. Hashimoto、 金 美羅、 辻 秀典、 田中 英彦、 情報処理学会論文誌、 Vol.51、 No.9、 pp.1682-1691、 情報処理学会 (2010).
2. “アプリケーションの実行状況に基づく強制アクセス制御方式”、 原田 季栄、 半田 哲夫、 M. Hashimoto、 田中 英彦、 情報処理学会論文誌、 Vol.53、 No.9、 pp.2130-2147 (2013).
3. “論理型言語による強制アクセス制御の実用的な実装に向けて”、 M. Hashimoto、 滝澤 峰利、 高 山 扶美彦、 辻 秀典、 田中 英彦、 信学技報、 vol. 115、 no. 334、 ICSS2015-44、 pp. 55-60 (2015).

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Yamauchi Toshihiro、Akao Yohei、Yoshitani Ryota、Nakamura Yuichi、Hashimoto Masaki	４．巻 0
２．論文標題 Additional kernel observer: privilege escalation attack prevention mechanism focusing on system call privilege changes	５．発行年 2020年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 0
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-020-00514-7	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 M. Kadoguchi, H. Kobayashi, S. Hayashi, A. Otsuka and M. Hashimoto
２．発表標題 Deep Self-Supervised Clustering of the Dark Web for Cyber Threat Intelligence
３．学会等名 2020 IEEE International Conference on Intelligence and Security Informatics (ISI)（国際学会）
４．発表年 2020年

１．発表者名 H. Kobayashi, M. Kadoguchi, S. Hayashi, A. Otsuka and M. Hashimoto
２．発表標題 An Expert System for Classifying Harmful Content on the Dark Web
３．学会等名 2020 IEEE International Conference on Intelligence and Security Informatics (ISI)（国際学会）
４．発表年 2020年

１．発表者名 M. KADOGUCHI, S. HAYASHI, M. HASHIMOTO and A. OTSUKA
２．発表標題 Exploring the Dark Web for Cyber Threat Intelligence using Machine Leaning
３．学会等名 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 2019, pp. 200-202, doi: 10.1109/ISI.2019.8823360.（国際学会）
４．発表年 2019年

１．発表者名
神田敦，橋本正樹

２．発表標題
乱数性を用いたTLS通信の識別

３．学会等名
コンピュータセキュリティシンポジウム2019論文集,2019,683-690（2019-10-14）.

４．発表年
2019年

１．発表者名
青柳守俊，辻秀典，橋本正樹

２．発表標題
ニューラル機械翻訳モデルを用いた異なるアーキテクチャ間における類似バイナリコードの検索

３．学会等名
研究報告セキュリティ心理学とトラスト（SPT）,2020-SPT-36(8),1-6（2020-02-24），2188-8671.

４．発表年
2020年

１．発表者名
井上仁人，橋本正樹

２．発表標題
HTTPリクエストの調査と偽のUser-Agent値の識別方法の提案

３．学会等名
研究報告セキュリティ心理学とトラスト（SPT）,2020-SPT-36(16),1-6（2020-02-24），2188-8671.

４．発表年
2020年

１．発表者名
小林華枝，橋本正樹

２．発表標題
ダークウェブ上に蔓延する違法有害情報の自動分類エキスパートシステムの開発

３．学会等名
研究報告セキュリティ心理学とトラスト（SPT）,2020-SPT-36(20),1-6（2020-02-24），2188-8671.

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	松井　俊浩 (Matsui Toshihiro) (90358010)	情報セキュリティ大学院大学・その他の研究科・教授 (32721)	
研究分担者	辻　秀典 (Tsuji Hidenori) (90398975)	情報セキュリティ大学院大学・その他の研究科・教授 (32721)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関