環境選択型マルウェアの挙動解析による自動対策システムの研究

２０１６年度　先端数理科学研究科

博士学位請求論文（要旨）

環境選択型マルウェアの挙動解析による自動対策システムの研究

現象数理学専攻
仲小路　博史

１　問題意識と目的

近年，コンピュータウイルス等のマルウェアが高度化し，マルウェアの侵入，感染を防ぎきることが困難と言われている．そこで感染を前提とした多層防御による対策が重要視されている．多層防御を実現するには，日々変化するマルウェアの挙動を解析して，その影響を最小限に抑える必要がある．解析手法としてマルウェアをサンドボックスという解析環境で実際に動かしてその挙動を解析する動的解析手法が普及している．ところが攻撃者もこれに対抗して，狙った環境でしか動作しないような解析回避機能が実装されたマルウェア（環境選択型マルウェア）が増加し，簡単には解析できない問題があった【問題１】.

このように高度化する攻撃者らはさらに連携しながら攻勢を強めてきている．我々守る側も単独組織による対策ではなく,組織間で解析結果等の脅威情報を共有して攻撃に備える集団防御の実現が求められている．一部ではマルウェアを解析して得た攻撃に悪用されるサイト情報を共有して，そこに対するインターネット接続を即座に遮断する自動対策技術も実用化されている．ところがマルウェアの中には，例えば検索エンジン等の正規のサイトにアクセスする種も存在するため，本技術を適用すると突然検索エンジンが使えなくなる等，業務に悪影響を及ぼすため導入に踏み切れず結果的に対策が後手に回る問題があった【問題２】.

本論文では高度なマルウェアを利用した標的型攻撃に対する早期対策の重要性に鑑み，業務への影響を考慮した自動対策システム「自律進化型防御システム（AED：Autonomous Evolution of Defense）」を提案し，環境選択型マルウェアへの自動対策を実現する．ここで前述した２つの問題に対応して以下を目的とする．

【目的１】挙動の解析が困難になってきている環境選択型マルウェアの増加という問題１に対して，環境選択型マルウェアを自動解析し，攻撃者による遠隔操作や情報搾取を防止するために有用となる“マルウェアの接続先（不審サイト）”を抽出.

【目的２】抽出した情報には不確実な情報も含まれているため，その情報をそのまま自動対策（遮断）に利用すると，ユーザの業務に悪影響を与えてしまう問題２に対して，マルウェアによる被害発生リスクの軽減と，誤った情報を用いて実施した自動対策による利用者の業務悪影響軽減を両立.

２　構成及び各章の要約

1 章では研究の背景と目的を述べる．2 章では，環境選択型マルウェアの挙動を自動的に解析して，マルウェアの通信先を抽出する基本手法を提案する．3 章では解析中にマルウェアをインターネットにアクセスさせて安全かつ高精度に解析する技術，4 章では一般的に推奨されている対策（認証付きプロキシ）をすり抜けるマルウェアを解析する技術をそれぞれ提案する．5 章は，2 章で提案したシステムを社会実装するにあたり弊害となるコスト増大の問題を解決する手法について述べる．6 章では解析対象をマルウェア（ファイル）から URL（Web サイト）へ拡張し，対処可能なアタックベクタ（攻撃経路）の拡大を図る.

これまで述べた技術により抽出したマルウェアの解析結果を用いて，ユーザの本来業務への悪影響を最低限に抑えた自動対策手法について 7 章で述べる．8 章では，本論文をまとめている.

1 章要約（研究背景と目的）

目的を達成するための課題を設定した．まず目的１に対し，環境選択型マルウェアの挙動を解明可能な動

的解析の実現【課題１】と，動的解析で一般的に利用されているインターネット隔離環境では現れない機能の把握【課題２】を設定した．また目的２に対し，マルウェアによる不正なアクセスの遮断【課題３】と，誤った情報による対策であったとしても業務上必要なアクセスは許可すること【課題４】を設定した．

2 章要約（マルウェア挙動解明）

環境選択型マルウェアへの対策に有用な情報“マルウェアの接続先（不審サイト）”を得るために，多種環境でマルウェアを解析する多種環境マルウェア動的解析システム（M3AS）を提案した．マルウェアが感染しやすい環境（解析エンジンや OS，アプリケーション）を，公開されている脆弱性の数を基準として選定することで，感染（観測）しやすいサンドボックスを構成した．本システムを用いてマルウェア 633 種を解析し，マルウェア対策に有用なマルウェアの接続先6,542URLを取得した．これにより課題１を解決した．

3 章要約（マルウェア通信制御）

インターネットと隔離された環境では動作しないマルウェアの機能の把握するため，閉塞環境で解析していた前記 M3AS を拡張し，第二のマルウェアのダウンロード通信のみ限定的にインターネットに接続させて解析精度を向上させる手法を提案した．評価により 644 種のマルウェアから 58 の第二のマルウェアの取得に成功し，さらに解析中に外部への攻撃がなかったことを確認することで，外部への攻撃を行うことなく，組織に侵入したマルウェアの特性を解明できることを明らかにした．これにより課題２を解決した．

4 章要約（プロキシアクセス型マルウェア解析）

多層防御における出口対策として導入が推奨されている認証付プロキシをも突破するマルウェア（プロキシアクセス型マルウェア）が増加している懸念から，M3AS を拡張してプロキシアクセス型マルウェアのプロキシ対応能力を判定するプロキシ認証突破判定システムを提案した．本システムを用いて，2014 年 10 月に取得したマルウェア 629 種を解析し，そのうち 84 種がプロキシ利用するプロキシアクセス型マルウェアで，8 種がプロキシ認証をも突破するマルウェアであることを確認した．

5 章要約（サンドボックス最適化）

M3AS はサンドボックス数と解析精度にトレードオフの関係があり，サンドボックスの拡充（精度向上）がコスト高騰に直結する．このためサンドボックスの個数と顕現（マルウェアがいずれかのサンドボックスで動作）の成否の関係を検証し，少ないサンドボックスでより多くのマルウェアを顕現可能なサンドボックス選定方式を提案した．評価の結果，本方式を適用してサンドボックスの数を 76 個から 27 個に減らした場合でも，すべてのマルウェアを顕現させられることを確認し，サンドボックス数を約 65%削減できた．

6 章要約（不正サイト挙動解明）

M3AS を拡張して不正サイトを解析するシステムを提案した．解析対象サイトへのアクセスに用いるブラウザ等の環境にバリエーションを持たせたサンドボックスを新たに構築し，不正サイトへアクセスするブラウザによって応答を変化させる巧妙な不正サイト（クローキング）の解析に対応した不正サイト挙動解明システムを開発した．代表的なブラウザ 4 種をインストールしたサンドボックスを用いて，実際に不正サイトの疑いのある 2,439 サイトを解析し，ブラウザによって挙動を変化させる不正サイトの存在を確認した．

7 章要約（挙動に基づく自動対策）

M3AS により得たマルウェアの接続先（不審 URL）を用いて，マルウェアによる不正なアクセスの遮断を実現する自動対策システムを考案した．不審 URL へ端末がアクセスする際に，人間と機械とを判別可能な CAPTCHA 認証を端末に対して与えることで，マルウェアによる機械的なアクセスのみ遮断する自律進化型防御システム（AED）を提案した．M3AS 等から得た 52,653 種類のユニークな不審 URL リストと AED を用いて評価した結果，2,064 種類のマルウェアの 99%以上の遮断に成功し，課題３を解決した．また，実証実験に参加した被験者に対して実施したアンケート結果では，誤った情報に基づく本提案手法による自動対策に「不便を感じた」と回答した被験者は 0 であった．これによって課題４を解決した．

以上，４つの課題を解決するための手法提案，実装，実験評価を通し，環境選択型マルウェアを自動解析して対策に有効な情報を抽出することで目的１を達成し，この情報に「業務へ悪影響を与える情報」が含まれていたとしても業務への影響を最低限に抑えて迅速，自動的に対策することで目的２を達成した．