セキュリティ対処の影響を考慮した自動対処システムの提案

重本 倫宏[†1,2]　藤井 康広[†1]　菊池 浩明[†2]

概要：近年，高度化されたマルウェアによるサイバー攻撃の被害が増加している．これらの脅威による被害の拡大を防ぐためには，マルウェアの攻撃手法を解明し，迅速に対処することが重要となる．攻撃手法を解明する手段として，マルウェアを動的解析する技術が存在する．しかし，動的解析結果にはマルウェアがネットワーク接続の有無を確認するために接続する正規の接続先が含まれる場合があり，そのまま対処に用いると業務に悪影響を与える場合がある．本報告では，組織における過去の接続ログから対処を適用した際の影響を自動的に算出し，算出した影響度に基づき自動対処を行うシステムを提案する．さらに，プロトタイプを用いた評価実験により，提案システムの有効性を示す．

キーワード：セキュリティ，マルウェア，動的解析，自動対処

Proposal of Automated Defense System based on Business Impact Analysis

Tomohiro Shigemoto[†1,2]　Yasuhiro Fujii[†1]　Hiroaki Kikuchi[†2]

Abstract: In recent years, the damage from cyber-attacks caused by sophisticated malware has increased. In a situation such as this, it is necessary to clarify the characteristics of the malware so that countermeasures can be taken quickly to prevent the damage from expanding. A dynamic analysis method is used in order to clarify the malware's behavior. However the dynamic analysis results sometime contain benign site used by malware's verifying network communication. So if block the malware communication listed in analysis results, thus it has caused disruptive effects on business. In this paper, we propose Automated Defense System based on business impact analysis. Proposed system evaluates business impact from connection log and decide whether to block communication or not.

Keywords: Security, Malware, Dynamic Analysis, Security Automation

1. はじめに

近年，民間企業や政府機関，制御システム等の重要インフラを狙ったサイバー攻撃が激化しており，個人，企業，国家それぞれの利益や安全性を損なうリスクが高まっている．特に APT（Advanced Persistent Threat）攻撃[1]は，秘密裏に，そして執拗に長期間攻撃を続ける点で従来の脅威とは異なり，マルウェアの侵入を検知あるいは防止することは不可能になりつつある．例えば，2015 年 6 月に日本年金機構において，遠隔操作型マルウェアに感染した職員の端末から基礎年金番号を含む個人情報が約 125 万件漏えいし，大きな社会問題となった[2]．従来のマルウェア対策は主に，セキュリティベンダなど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により行なわれている．アンチウイルスソフトは既知のマルウェアに対しては有効であるが，次々と発生する未知のマルウェアや高度な検知防止機能を持つマルウェアに対しては，ベンダ側でのマルウェア解析やシグネチャ作成が追いつかず，現状では十分対応しきれていない[3]．このような状況下においては，次々と発生するマルウェアの挙動を解明し，セキュリティ対策に繋げることが重要となってきている．

筆者らはこのような状況に鑑み，多種環境を用いて未知マルウェアの挙動を自動的に解明する，マルウェア動的解析システム（M3AS: Multi-modal Malware Analysis System）の研究開発を進めてきた[4][5]．M3AS を用いることにより，マルウェアの挙動解析を行うオペレータの負荷を大幅に削減しながら，マルウェアの接続先を抽出することが可能となる．しかし，マルウェアの中には，ネットワーク接続の有無を確認するために正規の接続先へ通信を行うものや，適当なドメインや IP アドレスにアクセスするなどの偽装工作を行うものも存在[6]し，動的解析の結果得られた接続先をすべて遮断すると業務に悪影響を与える場合がある．

本研究の目的は，マルウェア動的解析結果を活用したセキュリティ対処の自動化である．本報告では，自動対処を実現するにあたっての課題を分析し，自動対処システムに求められる要件を導出する．さらに，導出した要件に基づき自動対処システムを提案する．また，提案した自動対処システムを用いた評価実験を行い，提案システムの有効性を評価する．

†1 (株)日立製作所
Hitachi Ltd.
†2 明治大学
Meiji University

2. 関連研究

淵上ら[7]は，組織内に流入する実行ファイルをサンドボックスで実行し，感染拡大の原因となる活動が観測された時点で，感染拡大に伴う通信を遮断する設定を組織内ネットワークスイッチの ACL に追加することで, 感染拡大を抑制するネットワーク型動的解析システムを提案している．しかし，マルウェアが疎通確認のために行う正規サイトへの通信や，サンドボックス環境に導入した OS や，アプリケーションが行う正規の通信などが発生した場合には，誤って制御してしまうという問題が発生する．

著者らは，上記問題を解決するため，マルウェアの動的解析結果の情報や，共有されたインテリジェンスを活用することでサイバー攻撃に対して集団防御を実現する自律進化型防御システム（AED: Autonomous Evolution of Defense）の研究を進めている[8][9]. 我々の研究グループが提案する AED は，このような不確実性の高い脅威情報を用いて対策を実現するシステムである．具体的には，マルウェアの動的解析や共有されたインテリジェンスから得られた不審サイト情報をグレーリストとして管理し，クライアントがその不審サイトへアクセスしようとした場合に，プロキシで追加認証を要求する．これにより，例え誤った情報による認証追加であったとしても人間による業務上必要なアクセスは許可しつつ，マルウェア等の機械によるアクセスを遮断することを可能とする．しかし，AED では OS やアプリケーションが行うバックグラウンド通信の接続先がグレーリストに登録されてしまった場合に追加認証を突破できず, 誤って制御してしまう．

本稿で提案する自動対処システムは，これらの課題を解決するものであり，AED と組み合わせることで，より業務への悪影響を低減することが可能となる．AED との組み合わせ方については，5.4 節で考察する．

3. 自動対処システムの提案

3.1 自動対処における課題

マルウェアを動的解析して得られた解析結果に基づき自動対処を実現する際の課題を以下に示す．

【課題 1】解析結果にノイズが含まれている

マルウェア動的解析システムは，解析環境においてマルウェアを実行した際の通信先等の挙動を観測し解析結果として出力する．しかし，マルウェアの中には，ネットワークの疎通確認を行うために，正規サイトへアクセスを行うものが存在する．また，マルウェアの実行中に解析環境にインストールされた OS やアプリケーションが行う正規の挙動が解析結果に含まれる場合もある．このような解析結果のノイズにより正規サイトへの通信を誤って遮断してしまう場合がある．

【課題 2】対処すべき機器や対処方法が分からない

解析結果に含まれる挙動から，どの機器でどのような対処をすれば良いか分からない．また，たとえ対処方法が分かっていたとしても，対処の適用がバッチ処理で行われることにより, 通信遮断までのタイムラグが発生してしまう．

【課題 3】業務を止められない

セキュリティ対処を適用することにより，業務にどのような影響がでるか分からない．このため，業務影響を調査しなければならず，この調査に時間を要する．

これらの課題から，マルウェア自動対処に求められる要件を整理した．以下に，自動対処システムに求められる要件を示す．

【要件 1】解析結果のノイズを除去すること

解析結果に含まれる正規サイトの情報や，OS やアプリケーションが行う正規の挙動を除去すること．

【要件 2】機器に適用可能な脅威を抽出すること

セキュリティ機器ごとに適用可能な脅威を抽出し，自動で対処すること．

【要件 3】対処した際の影響を評価すること

対処した際に発生する業務への影響を見積もり，影響度に応じて自動対処の可否を設定できること．

3.2 自動対処システムの提案

3.1 節で整理した要件に基づき，自動対処システムを提案する．以下に各要件に対する対応方針を述べる．

【要件 1】への対応として，脅威情報の評価を行う機能を開発する．脅威情報の評価では，外部のセキュリティベンダの情報等を参考に，脅威情報の確信度（当該脅威情報がどれだけ信頼できるかの指標）を算出する．なお，確信度の算出方法は 4.2 節で述べる．

【要件 2】への対応として，マルウェア解析結果からセキュリティ機器に適用可能な脅威情報（例えば，マルウェアが接続を行うドメインや IP アドレス等）を抽出する機能と，組織に配備されているセキュリティ機器ごとに脅威情報を受け取り，対処を自動適用する機能（以下，アダプタ）を開発する．

【要件 3】への対応として，対処影響の評価を行う機能を開発する．対処影響の評価では，これまでの業務活動の情報を参考に，業務への影響度（当該対処の適用によってどれだけ業務が阻害されるかの指標）を算出する．なお，影響度の算出方法は 4.2 節で述べる．

提案する自動対処システムの概要を図 1 に示す．

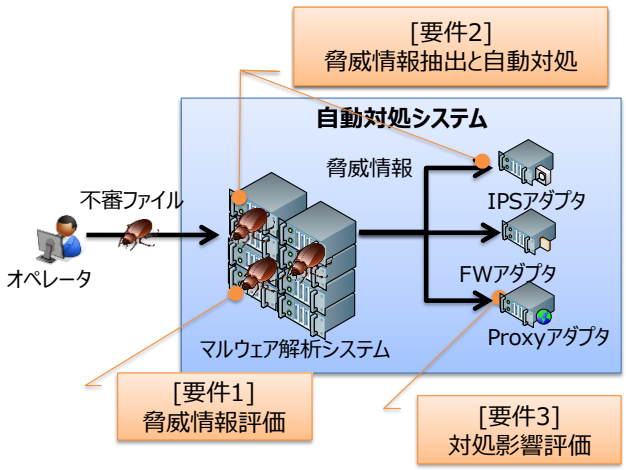

図 1　自動対処システムの概要

Figure 1　Overview of Automated Defense System.

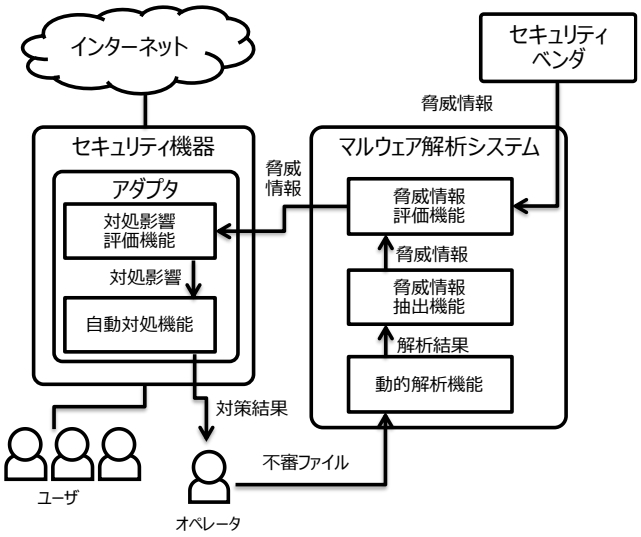

図 2　自動対処システムの構成

Figure 2　Architecture of Automated Defense System.

自動対処システムの具体的な処理の流れを説明する．

1. オペレータは，不審検体をマルウェア解析システムに投入する．
2. マルウェア解析システムは，投入された不審検体を動的解析し，対処に適用可能な脅威情報を抽出する．
3. マルウェア解析システムは，抽出した脅威情報の確信度を算出する．
4. マルウェア解析システムは，確信度が付与された脅威情報を，影響度評価のため，セキュリティ機器と共有する．
5. セキュリティ機器は，マルウェア解析システムから共有された脅威情報を受信し，対処を適用した場合の業務への影響度を算出する．
6. セキュリティ機器は，脅威情報に付与された確信度と，対処を適用した場合の影響度とから，対処の適用可否を判断し，適用が可能な場合は対処する．

このように，マルウェアの解析結果から脅威情報を抽出し，脅威情報の確信度と，対処した場合の影響度を用いることで，業務影響を考慮した自動対処を行うことが可能となる．次章では，自動対処システムの詳細について述べる．

4. 自動対処システムの設計

4.1 自動対処システムの概要

提案する自動対処システムの構成を図 2 に示す．

提案する自動対処システムは，以下 5 つの機能から構成される．

(1) **動的解析機能**

投入された不審検体を動的解析する機能．

(2) **脅威情報抽出機能**

動的解析の解析結果から脅威情報を抽出する機能．セキュリティ機器に適用可能な脅威情報を抽出する．

(3) **脅威情報評価機能**

抽出した脅威情報の確信度を算出し，確信度を付与した脅威情報を共有する機能．なお，マルウェア解析システムと各セキュリティ機器での脅威情報の共有は，サイバー攻撃活動を記述するための仕様である STIX（Structured Threat Information eXpression）[a]を用いて行う．

(4) **対処影響評価機能**

脅威情報を受け取り，対処を実行した際の影響度を評価する機能．セキュリティ機器ごとに影響度を評価するアダプタを開発する．

(5) **自動対処機能**

確信度と，影響度を基に自動で対処を適用する機能．なお，セキュリティ機器ごとに対処を適用するアダプタを開発する．

4.2 自動対処システムの詳細

本節では，提案システムを構成する機能の詳細を説明する．

(1) **動的解析機能**

動的解析機能では，マルウェアをサンドボックス環境で実行し，マルウェアの挙動を明らかにする．なお，マルウェアの挙動を解析する動的解析製品として，Fire Eye[10]や，

a) http://stixproject.github.io/

ThreatAnalyzer[11]などが存在する．また，OSS(Open Source Software)では Cuckoo Sandbox[12]が入手可能である．提案する自動対処システムでは，筆者らが開発している，多種環境でマルウェアの解析を行う M3AS を活用する．

(2) 脅威情報抽出機能

脅威情報抽出機能では，動的解析機能が出力した解析結果から，セキュリティ機器に適用可能な脅威情報を抽出する．組織で活用されている主なセキュリティ機器で対処に活用できる脅威情報を表 1 に示す．なお，括弧内には，セキュリティ機器を実現する代表的なオープンソースのソフトウェアを示す．

表 1　セキュリティ機器で利用可能な脅威情報

Table 1　Available Threat Information for Security Devices.

	プロキシ（Squid[b]）	IPS（Snort[c]）	FW（iptables[d]）
IP アドレス	○	○	○
ドメイン	○	○	×
URL	○	○	×
User-Agent	○	○	×
コンテンツ	×	○	×

例えば，プロキシで対処を行う場合には，IP アドレスや，ドメイン，URL，ユーザエージェントの脅威情報を抽出し，共有する．

(3) 脅威情報評価機能

1 章で述べたように，解析結果から抽出した脅威情報には正規サイトや正規の挙動情報が含まれる場合がある．脅威情報評価機能では，脅威情報に確信度を付与することで，これら正規サイトや正規の挙動を誤って遮断してしまうことを抑制する．脅威情報評価機能では，抽出した脅威情報に対して，セキュリティベンダ等の外部のデータベースを参照し確信度を算出する．提案する自動対処システムでは，VirusTotal[e]を参照し，確信度として High，Middle，Low，None，Unknown のいずれかを出力する．VirusTotal とはユーザが投稿された検体や，ドメイン，URL を複数のウイルス対策ソフトや，Web サイトスキャナなどを用いて解析した結果を返すサービスである．提案手法では，悪性（ポジティブ）と判断した Web サイトスキャナの数に応じて確信度を算出する．なお，評価対象の脅威情報が VirusTotal に登録されていない場合は，確信度「Unknown」を出力する．VirusTotal を用いた確信度の設定例を表 2 に示す．

表 2　VirusTotal を用いた確信度設定

Table 2　Confidence Configuration using VirusTotal.

確信度	悪性と判断した WEB スキャナの数
None	0
Low	1
Medium	2
High	3 以上
Unknown	-

さらに，脅威情報評価機能は，脅威情報を STIX として出力する．STIX で出力することで，提案システム以外の STIX を活用したセキュリティ機器との連携も可能となる．図 3 に脅威情報の出力例を示す．

```
<?xml version="1.0"?>
- <stix:STIX_Package version="1.2" id="example:Package-023b27dd-
083f-4563-9258-4efa0056e1a9"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:example="http://example.com"
xmlns:URIObj="http://cybox.mitre.org/objects#URIObject-2"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:indicator="http://stix.mitre.org/Indicator-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:stix="http://stix.mitre.org/stix-1">
  - <stix:STIX_Header>
      <stix:Description>M3AS:STIX</stix:Description>
    </stix:STIX_Header>
  - <stix:Indicators>
    - <stix:Indicator id="example:indicator-d8e915a9-b215-42ba-
      96e4-f81e6455fe8e" xsi:type="indicator:IndicatorType"
      timestamp="2017-07-20T04:29:15.688158Z">
        <indicator:Type
          xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
          Watchlist</indicator:Type>
      - <indicator:Observable id="example:Observable-4878bc33-
        9f54-4f6f-8a76-26fc87895824">
        - <cybox:Object id="example:URI-3d155515-d634-48e1-
          9d3f-9c2bc976bad6">
          - <cybox:Properties type="Domain Name"
            xsi:type="URIObj:URIObjectType">
              <URIObj:Value>apartments-
                gurgaon.com</URIObj:Value>
            </cybox:Properties>
          </cybox:Object>
        </indicator:Observable>
      - <indicator:Confidence timestamp="2017-07-
        20T04:29:16.606258Z">
          <stixCommon:Value>High</stixCommon:Value>
        </indicator:Confidence>
      </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

図 3　脅威情報の例

Figure 3　Example of Threat Information.

(4) 対処影響調査機能

対処影響調査機能では，脅威情報を受け取り，対処を適用した際の影響度を評価する．対処影響調査機能はセキュリティ機器ごとに実装する．例えば，Proxy（Squid）の場合は，アクセスログを参照し，脅威情報として出力されたドメインへのアクセス割合を算出し，影響度とする．なお，アクセスログを SIEM や DB に格納している場合は，そこから影響度を算出してもよい．

また，FW で対処を適用した場合の影響度を算出するには，FW を通過するログを記録する設定で運用しておく必要がある．IPS は，通常シグネチャにマッチしたログのみ

b) http://www.squid-cache.org/
c) https://www.snort.org/
d) https://www.netfilter.org/index.html
e) https://www.virustotal.com/ja/

を記録する．このため，IPS で対処を適用した場合の影響度を算出するには，脅威情報に含まれるシグネチャを生成し，その後，一定期間運用した後に算出しなければならない．ただ，表 1 で示したように，他のセキュリティ機器から影響度を算出することもできる．例えば，Proxy を運用していれば，IP アドレス，ドメイン，URL，ユーザエージェントの情報をログに記録することができ，そこから FW や，IPS で対処を適用した場合の影響度を算出してもよい．

(5) 自動対処機能

自動対処機能では，脅威情報，確信度，対処影響度を受け取り，対処の適用可否を決定し，セキュリティ対処を実行する．対処適用の設定例（自動対処を行う確信度と対処影響度の組合せ）を表 3 に示す．なお，この設定値は運用に応じて変化させてもよい．

表 3　自動対処の設定
Table 3　Automatic Response Configuration.

確信度	対処影響度
None	0%
Low	1%以下
Medium	5%以下
High	10%以下
Unknown	3%以下

確信度が高ければ，対処による影響がありそうな場合でも対処を自動適用するが，確信度が低ければ対処による影響が出そうな場合に自動適用しないように設定することができる．上記設定例は，確信度が High の場合は対処により 10%の通信に影響が出る場合でも対処を自動適用することを表している．

5. 評価実験

提案手法の有効性評価のため，自動対処システムのプロトタイプを実装し，評価した．本章では，開発した自動対処システムの評価実験について述べる．なお，プロトタイプでは，プロキシのアダプタを実装し，マルウェアの接続先ホストを脅威情報として抽出した．

5.1 評価目的

開発した自動対処システムを以下の観点で評価する．

(1) 自動対処速度について

検体の解析から自動対処までの時間を評価する．

(2) 自動対処精度について

マルウェア解析結果から得られた脅威情報のうちどの程度が自動対処されるかを評価する．

(3) 確信度のみと影響度のみを用いた自動対処について

マルウェア解析結果から得られた脅威情報を確信度のみを用いて対処した場合と，影響度のみを用いて対処した場合，確信度と影響度を用いて対処した場合（提案手法）の 3 パターンについて，どの程度が自動対処されるかを評価する．

(4) 影響度評価に用いるユーザ数と期間について

対処影響調査機能において，業務情報として利用するユーザ数を n 人, 利用する期間を N 日とし, n と N および FPf（フォールスポジティブ）の関係を評価する．

5.2 評価方法

(1) 自動対処速度について

提案システムのプロトタイプを用いて 100 検体を解析し，各機能の処理にかかる時間を計測する．

(2) 自動対処精度について

提案システムのプロトタイプを用いて 732 検体を解析し，抽出した脅威情報の確信度を評価する．また，ある組織におけるプロキシのアクセスログを用いて脅威情報のうちどの程度が自動対処されるかを机上検討する．表 4 に評価に用いたプロキシログの情報を示す．

表 4　プロキシログの概要
Table 4　Proxy Log.

項目	値
ユーザ数	34 ユーザ
期間	2016/2/25-3/5
アクセス総数	543,914 アクセス
接続先ホスト数（ユニーク）	5,110 ドメイン

(3) 確信度のみと影響度のみを用いた自動対処について

「(2)自動対処精度について」で用いた検体およびプロキシアクセスログを用いて，確信度「None」の脅威情報を自動対処の対象外した場合と，影響度が 0 より大きい（一度でもアクセスがある）脅威情報を自動対処の対象外とした場合，提案手法の 3 パターンについて，自動対処される脅威情報の数と，業務影響が存在する脅威情報の数を評価する．

(4) 影響度評価に用いるユーザ数と期間について

業務情報として利用するユーザ数（n=1,17,34）と期間（N=1,3,7）について FP を評価する．評価には，「(2)自動対処精度について」で用いた検体およびプロキシアクセスログを用いる．また，自動対処した脅威情報のうち，評価対象期間（34 ユーザのプロキシログ 3 日分）にアクセスが観測された脅威情報の割合を FP として評価する．

5.3 評価結果

(1) 自動対処速度について

各機能の 1 検体あたりの平均処理時間を表 5 に示す．

f) 正常な通信を誤って異常と検知し、遮断してしまう割合

表 5　自動対処システムの処理時間

Table 5　Processing Time of Automatic Response System.

機能	処理時間[秒]
動的解析機能	460
脅威抽出機能	0.14
脅威評価機能	2.6
対処影響評価機能	1.0
自動対処機能	0.54
計	464.28

1 検体あたりの平均処理時間は約 464 秒となった.

(2)　自動対処精度について

732 検体から脅威情報（不審ホスト）は 3,739 ホスト抽出された. なお, ユニークな脅威情報は 508 ホスト存在し, そのうちの 491 ホストが自動対処の対象となった. 確信度別の脅威情報抽出数及び, 対処影響数, 自動対処対象数を表 6 に示す. ここで, 対処影響数とは, 影響度が 0%以上の（評価に用いたプロキシログで, 1 度でも接続が確認された）脅威情報の数を表す.

表 6　評価結果

Table 6　Evaluation Result.

確信度	脅威情報数	対処影響数	自動対処数
None	132	17	115
Low	118	2	118
Medium	80	0	80
High	159	0	159
Unknown	19	0	19
計	508	19	491

表 6 より, 確信度 None の脅威情報のうち, 対処影響が確認された 17 件が自動対処の対象外となったことが分かる. また, 確信度 Low の脅威情報のうち, 2 件は対処影響が確認されたが, 影響度が少なかったため, 自動対処の対象となったことが分かった. なお, 確信度 Low で対処影響が確認された接続先は, 短縮 URL サイトと, CDN（Content Delivery Network）で利用されているドメインであった.

(3)　確信度のみと影響度のみを用いた自動対処について

確信度「None」の脅威情報を自動対処の対象外した場合と, 影響度が 0 より大きい（一度でもアクセスがある）脅威情報を自動対処の対象外とした場合, 提案手法の 3 パターンについて自動対処数と, 自動対処によって業務へ影響が出る脅威情報の数（対処影響数）の関係を表 7 に示す.

表 7　自動対処数と影響数

Table 7　Number of Automatic Response and Impact.

	自動対処数	対処影響数
確信度のみ	376	2
影響度のみ	489	0
提案手法	491	2

表 7 より, 提案手法は 3 パターンのうちで最も多く自動対処を実施していることが分かる. 対処影響度のみを用いて自動対処を行う場合, 影響数は 0 となるが, 確信度「Low」の脅威情報 2 件を対処することができない. 確信度と影響度を用いて柔軟に対処の設定を変更できる提案手法はこの点で確信度のみを用いた自動対処や影響度のみを用いた自動対処よりも優れていると考える.

(4)　影響度評価に用いるユーザ数と期間について

影響度評価時の業務情報として利用するユーザ数（n=1,17,34）と期間（N=1,3,7）を変化させた際の FP を図 4 に示す.

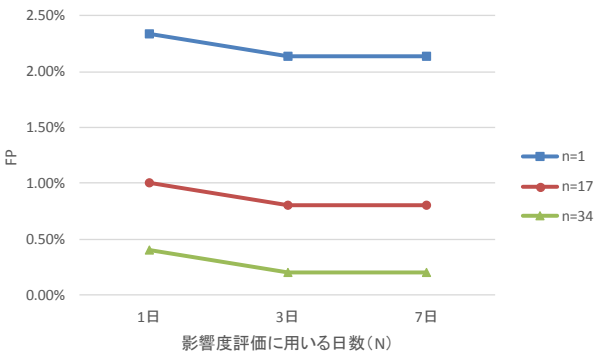

図 4　ユーザ数および期間と FP

Figure 4　FP rate with regard to the size of n and N.

図 4 より, 影響度評価に用いるユーザ数（n）が増えるほど, FP の値が低下することが分かる. また, 影響度評価に用いる日数は 3 日程度あれば十分であることも確認できた.

5.4　考察

(1)　AED との連携について

提案した自動対処システムの脅威情報適用先の一つとして, 筆者らが開発している AED を用いることで, 業務への影響をより低減できると考えられる. 具体的には, 確信度 None の脅威情報を AED で対処したり, 適用先が AED である場合には, 表 3 に示した自動対処設定の閾値を高く設定（対処影響が大きくても自動対処を行うよう設定）したりすることが考えられる.

(2)　対処漏れの可能性について

提案した自動対処システムでは, マルウェアを動的解析して得られた脅威情報を用いて対処を行う. 例えば, DGA（Domain Generation Algorithm）[13]を用いて解析の度に接続先を生成するマルウェアや, ランダムな接続先へ拡散を試みるマルウェアなどは, 動的解析で接続先全てを抽出することができず, 対処漏れを起こしてしまう可能性が発生する. 本問題については継続して対策方法を検討していく.

(3) **外部インテリジェンス情報との連携について**

近年，組織間でインテリジェンス（脅威情報や IT 機器の脆弱性情報およびそれらに関する分析や対処支援情報）を共有して攻撃に備える集団防御の概念が浸透しつつある．提案した自動対処システムでは，マルウェアの動的解析結果から得られた脅威情報を自動対処の対象としたが，これらのインテリジェンスから得られた脅威情報を用いて自動対処を実現することで，より多くの攻撃に対処できるようになると考えられる．

6. おわりに

本稿では，組織における過去の接続ログから対処を適用した際の影響を算出し，算出した影響度に基づき自動対処を行うシステムを提案した．さらに，プロキシと連携したプロトタイプを用いた評価実験により，464 秒でマルウェアの動的解析から対処適用までが完了すること，実マルウェアから 508 件の脅威情報を抽出し，そのうちの 491 件を自動対処できることを確認した．今後は，大規模環境での実証を通じて，精度向上を図る．

本稿中で使われているシステム・製品名は，各社の商標または登録商標です．

参考文献

[1] “標的型攻撃/新しいタイプの攻撃の実態と対策”. http://www.ipa.go.jp/files/000024542.pdf, (参照 2017-08-01).

[2] “「日本年金機構の情報漏えい事件から得られる教訓」公開のお知らせ”. https://www.lac.co.jp/news/2015/06/09_news_01.html, (参照 2017-08-01).

[3] “Antivirus software is dead, says security expert at Symantec”. https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec, (参照 2017-08-01).

[4] 仲小路博史，重本倫宏，鬼頭哲郎，林直樹，寺田真敏，菊池浩明．多種環境マルウェア動的解析システムの提案および評価．情報処理学会論文誌, vol. 56, No. 9, pp. 1730-1744, 2015.

[5] 重本倫宏，徳山喜一，下間直樹，鬼頭哲郎，明仲小路博史．マルウェア解析向け通信制御システムの開発．情報処理学会論文誌, vol. 57, No. 9, pp. 2012-2020, 2016.

[6] “サンドボックス回避手法への対策”. http://www.checkpoint.co.jp/threat-cloud/2016/10/defeating-sandbox-evasion-increase-successful-emulation-rate-virtualized-environment.html, (参照 2017-08-01).

[7] 淵上智史，長谷川皓一，山口由紀子，嶋田創，高倉弘喜．マルウェア感染拡大抑止に向けたネットワーク型動的解析システム．研究報告インターネットと運用技術(IOT). vol. 2016-IOT-32, no. 36, pp. 1-6, 2016.

[8] 仲小路博史，藤井康広，磯部義明，重本倫宏，鬼頭哲郎，林直樹，川口信隆，下間直樹，菊池浩明:人間行動を用いた自律進化型防御システムの提案，暗号と情報セキュリティシンポジウム 2016 (SCIS2016), pp 1-8(2016).

[9] H. Nakakoji, Y. Fujii, Y. Isobe, T. Shigemoto, T. Kito, N. Hayashi, N. Kawaguchi, N. Shimotsuma, H. Kikuchi, Proposal and Evaluation of Cyber Defense System Using Blacklist Refined Based on Authentication Results, 2016 19th International Conference on Network-Based Information Systems (NBiS), Ostrava, 2016, pp. 135-139.

[10] “サイバー・セキュリティとマルウェア対策”. https://www.fireeye.jp/, (参照 2017-08-01).

[11] “Dynamic Malware Analysis Tools, Malware Sandbox”. http://www.threattracksecurity.com/enterprise-security/malware-analysis-sandbox-software.aspx, (参照 2017-08-01).

[12] “Automated Malware Analysis”. http://www.cuckoosandbox.org/, (参照 2017-08-01).

[13] D. Plohmann, K. Yakdan, M. Klatt, J. Bader, E. Gerhards-Padilla, A Comprehensive Measurement Study of Domain Generating Malware, 25th USENIX Security Symposium (USENIX Security 16), Austin, 2016, pp. 263-278.