Computer Security Symposium 2017
23 - 25 October 2017

標的型に対する知的ネットワークフォレンジックシステム LIFT の開発と機能拡張 （その 4） －将来起こりうる攻撃方法の推定－

渋谷 健太[†1] 久山 真宏[†1] 松本 隆[†1] 八槇 博史[†1] 佐々木 良一[†1]

概要：近年，特定の企業や組織を攻撃対象とする標的型メール攻撃が問題となっている．このような攻撃に適切に対処するため，著者らは，ログ分析と人工知能などを用いて対策をガイドするシステムである LIFT（Live and Intelligent Network Forensic Technologies）の開発並びに機能拡張を行っている．従来の報告者らの研究で既存の攻撃に対しては正しく事象の推定が可能であることが明らかになったが，近い将来起こりうる攻撃に対し，適切に対応できるかどうかは明らかでない．そこで，本稿では先行するマルウェアと類似のマルウェアを取り上げ，VirusTotal を用いて亜種を収集し，亜種の発生パターンを比較することにより，将来発生しうるマルウェアの亜種の予測をこころみたので報告する．

キーワード：デジタルフォレンジック，ネットワークフォレンジック，標的型攻撃，マルウェア

Development and enhancement of intellectual network forensic system LIFT against targeted attacks (Part 4) -Estimation of future possible attack methods-

Kenta Shibuya[†1] Masahiro Kuyama[†1] Takashi Matsumoto[†1]
Hirofumi Yamaki[†1] Ryoichi Sasaki[†1]

Abstract: In recent years, targeted mail attacks targeting specific companies and organizations are becoming a problem. In order to cope with such attacks appropriately, the authors are developing and expanding functions of LIFT (Live and Intelligent Network Forensic Technologies) which is a system for guiding measures using log analysis and artificial intelligence. Conventional researchers' research has revealed that it is possible to estimate events correctly for existing attacks, but it is not clear whether we can respond appropriately to possible attacks in the near future. In this paper, we report malware that is similar to the preceding malware, collects subspecies using VirusTotal, and compares the occurrence patterns of subspecies, thereby predicting a possible subspecies of malware in the future.

Keywords: Digital Forensic, Network Forensics, Targeted attacks, Malware

1. はじめに

2016 年 6 月に起きた JTB における情報流出の被害事例に挙げられるように近年，特定の組織や個人を攻撃対象としたサイバー攻撃の一種である標的型攻撃が社会問題となっている．この標的型攻撃は，攻撃対象から機密情報や知的財産等の情報の窃取や破壊，改ざんを目的に行われる 攻撃である[1]．使用されるマルウェアは，攻撃者が事前に入手した標的の情報を元に従来のマルウェアをカスタマイズしたマルウェアが使用されることが多い[2]．このことから，マルウェアが流通することが少なく，検体の入手が困難であることからシグネチャの作成が困難であることが特徴として挙げられる[3].

このように従来のマルウェアに変更を加えたものは亜種と呼ばれる．こういった亜種を作成するためのツール[4]はブラックマーケットで開発ツールの取引が行われ，用意に入手が可能である[5]．開発ツールを使用することで，マルウェアに関する技術的な知識がなくても作成が容易に効率的になっている．このような要因もあり亜種はその数を爆発的に増加させている[6].

標的型攻撃の対策において，前述したようにマルウェアが攻撃対象に合わせてカスタマイズされている事で，シグネチャによる検知が困難である．加えて，亜種の出現数が増加していることからシグネチャの作成や定義ファイルの更新が亜種の登場に追いつかず，対策が後手に回っていることが現状の問題として挙げられる[7].

このような状況の中で，著者らは標的型攻撃に対処するため，各種ログや攻撃事象の特徴から人工知能技術を用いて応急対応のガイドや自動運転の支援を行う LIFT（Live and Intelligent Network Forensic Technologies）システムおよび，その機能拡張を行ってきた[8][9][10][11]．これにより，既に存在したマルウェアに対応したインシデントにおいて

†1 東京電機大学
Tokyo Denki University

は発生事象を正しく認識することができ，対応が可能であると示されている．

しかし，マルウェアの亜種の増加に伴い，現状の方式で増加する亜種に対応していくには，マルウェアの亜種を解析し，その都度検知に関するルールをチューニングする必要があり，対策が後手に回ることになる．

そこで本稿では，LIFT システムの拡張として未知の攻撃をシミュレート，対策を作成するためのデータとして，マルウェアの亜種が発生するパターンを分析し，今後発生する亜種に対する予測を行う．この予測を利用し，実際にマルウェアが出現する前に対策を行う事で，現状の後手に回っている対策に対し，先手を打つことを目的としている．

また，分析には数多く出現しているマルウェアの亜種の中でも，特に JTB における情報流出の際に使用された「PlugX」[12]に加え「Emdivi」，「POISONIVY」を対象とした．

マルウェアの収集には Virus Total[13]を使用し，オンライン型のサンドボックス製品である Lastline[14]を用いて解析を行った．そして，マルウェアごとの機能の変化を比較し，亜種の発生パターンから「PlugX」の今後発生する亜種の予測ができないか分析を行った．

本論文では，第 2 章で関連研究，第 3 章で先行研究，第 4 章で本研究をどのような手順で行うか，第 5 章で第 4 章の手順を行うことで得られた結果，第 6 章で考察，第 7 章で今後の展望について述べる．

2. 関連研究

マルウェアの亜種分析に関しての研究の多くは，分類をするための手法の提案を行い，その上で未知のマルウェアを分類・識別ことが出来るかといったものである[15][16]．

しかし，本研究が対象を標的型攻撃に使用された種別を選択しているように，用途を絞った研究はあまりされていない．また，今後出現するマルウェアがどういった機能を有しているかといった予測を行った研究は，我々の調査した範囲では見当たらない．

3. 先行研究

本研究に先行する研究として，著者らが所属する東京電機大学内の情報セキュリティ研究室およびサイバーセキュリティ研究所内で行なわれている LIFT システムおよびその機能拡張が挙げられる．

3.1 LIFT システム

LIFT（Live and Intelligent Network Forensic Technologies）システムとは，収集するべきログの管理や，徴候から人工知能技術を用いることで攻撃の推定，分析を行い，高い技術力を持たない組織であってもインシデント発生時に応急対応を支援することを目的としたシステムである[17]．

LIFTシステムの概要は図1の通りである．

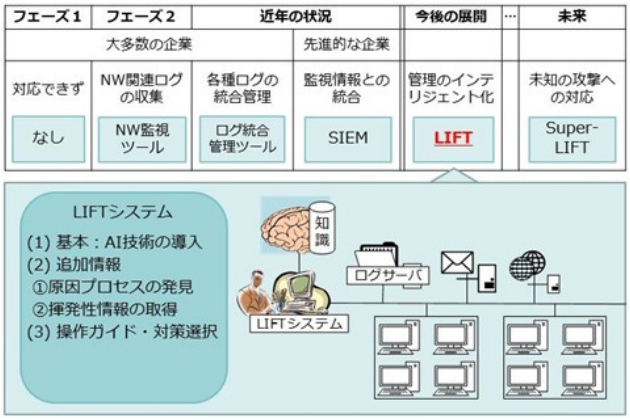

図 1　LIFT システムの概要

Fig.1　Overview of LIFT System.

LIFT システムの主な機能は，各種セキュリティ情報から現在行われている攻撃の徴候を検知することで，ベイジアンネットワークを利用した攻撃事象の推定機能を持つ.また推定した攻撃に対し，システム内の「事象・対策関連テーブル」を利用した対策の選択機能を持つ．このとき，攻撃事象の状況や選択された対策案によって運用者に対してガイドを表示する機能も用意されている．

LIFT システムの機能の概要を図 2 に示す．

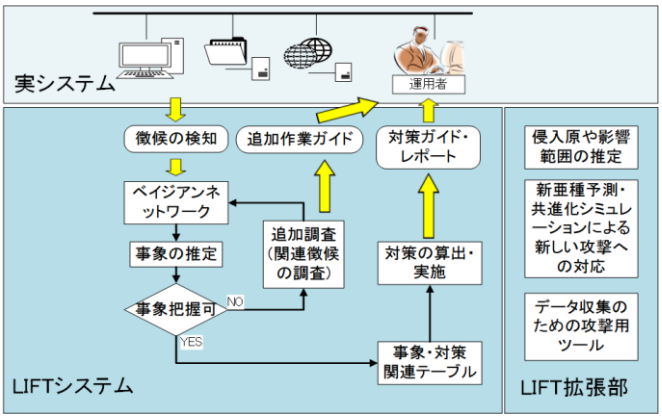

図 2　LIFT システムの機能概要

Fig.2　Functional Overview of LIFT System.

3.2 LIFT における機能拡張

LIFT プロジェクトでは，既に存在する攻撃のみならず，今後現れるとされる未知の攻撃においても対応を可能にするべく，マルウェアの侵入源や影響範囲の推定機能，新たな攻撃の予測機能，攻撃データ収集のための攻撃用ツールなどの LIFT システムの機能を拡張するための研究が行われている[18][19]．

本稿では，特に著者らが行っている新たな攻撃の予測機能に関して述べていく．

- 共進化モデルに基づく予測

  攻撃者に先回りする形で攻撃内容を自動合成してシミュレーションを行い，防御方法まで自動的に生成する．攻撃内容とそれに対する防御は，人工知能技術の一分野である進化計算を用いて行い，膨大な数の進化パターンを効率的に探索する．攻撃内容と防御手法がお互いに適応して進化する「共進化」の枠組みを取り入れ，その計算をクラウド上で行うことにより，ネットワーク内で起きうる攻撃とそれへの適切な防御とを求めることが可能となる．詳細に関しては文献[20]を参照されたい．

- **過去の発生パターン**に基づく予測

  対象マルウェアの亜種を動的解析することで取得した機能に関して，発生パターンを調査する．この調査を登場時期の異なる複数種別のマルウェアにおいて実施することで後続のマルウェアにおいて発生しうる機能の予測が可能となる．

  以降では，過去の発生パターンに基づく予測における手法の提案および予測結果の報告を行う．

4. 提案手法

本研究では，①標的型攻撃で使用されるマルウェアの亜種を収集し，②収集した検体についてサンドボックス環境での動的解析を行う．③動的解析により得られた結果から機能に関する情報を取得し，④発生パターンの調査，そこから亜種の機能の予測を行う．

4.1 マルウェアの収集

4.1.1 対象マルウェア

収集の対象となるマルウェアの選定は，Trend Micro 社の国内標的型攻撃レポート[21][22][23]に基づき，収集期間である 2015 年から 2017 年において使用率の高い種別のものとした．選定に用いたマルウェアの使用率は図 3 の通りである．

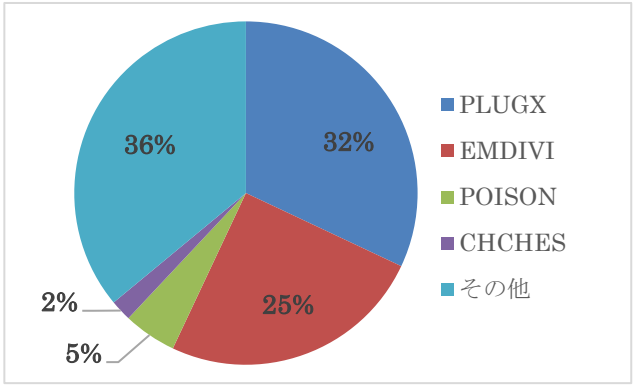

図 3 標的型攻撃におけるマルウェアの使用率

Fig.3 Malware usage rate in targeted attacks.

収集の対象としたそれぞれのマルウェアに関しては以下の通りである．

A) EMDIVI

日本年金機構における情報流出[24]をはじめとする被害事例において使用された種別のマルウェアである．2015 年の国内標的型攻撃レポートでは最も出現率の高かった検体であるが，現在では出現数が減っている．

B) PlugX

JTB における情報流出[12]をはじめとする被害事例において使用された種別のマルウェアである．2016 年以降の国内標的型攻撃レポートにおいては最も出現率が高いとされている．

C) POISON，POISONIVY

EMDIVI と PlugX よりも以前に出現している種別のマルウェアであり，比較を行う上で最適であると考えている．

D) ChChes

EMDIVI との類似されているマルウェアである．EMDIVI の出現数減少に際して，新たな比較対象として使用できると考えている．

4.1.2 収集方法

対象となるマルウェアの収集に際し，ファイル，URL のオンラインスキャンサービスである VirusTotal[13]を使用した．この VirusTotal では，40 種類以上のウィルス対策製品での検知結果を閲覧，検体の入手が可能となっている．

収集方法においてはキーワードによる検索機能にて各マルウェアの種別名を使用することで，VirusTotal 内のいずれかのウィルス対策製品該当するマルウェアとして検知された検体に関して収集を行うものとした．

4.2 マルウェアの解析

4.2.1 Lastline

lastline 社が提供する Lastline[14]というオンライン型サンドボックスの，特に検体を投稿することでサンドボックス環境での動的な解析が可能な Lastline Analyst という機能を使用することで検体の解析を行う．

この Lastline では，多くのセキュリティベンダーに利用されているバイナリファイル分析サービス「Anubis」や Web 脅威分析サービス「Wepawet」のナレッジが活用されている他，独自の手法で世界中の「活動している C&C サーバ」，「有害な IP アドレス」，「最新のマルウェア」，「エクスプロイトが埋め込まれたファイル」，「有害な Web サイト」，「マルウェアを配信しているサーバ」といった脅威情報を収集している．こういった多くの情報を利用して解析が行える事から信頼性の高い情報が得られるだけでなく，他の環境では得ることのできない情報についても収集可能であると考える．

4.2.2 Malwr

解析環境の違いによって得られる機能情報の有無についても予測に用いる要素とする．その為，オープンソースのマルウェア解析ツールである Cuckoo SandBox をベースとしたマルウェア分析サービス Malwr[25]についても同様に動的解析を行う．

4.3 解析結果の利用

分析には，Lastline Analyst より得られた解析情報をマルウェアの機能とし，検体が VirusTotal へ初めて投稿された日時情報をマルウェアの出現日時としてそれぞれ使用する．

マルウェアの出現日時として，検体を解析した結果から得られたタイムスタンプ情報でなく，VirusTotal から日時情報を利用した．これは，検体から得られた情報は攻撃者によって改ざんされている恐れがあるが，攻撃者の手から離れた VirusTotal 内の情報であれば改ざんの可能性が低いと考えたためである．

また分析で使用する機能は，今回使用する中でも最も使用率の高い「PlugX」の亜種からに得られた機能とした．対象とした機能が「EMDIVI」，「PlugX」，「POISONIVY」，「ChChes」の検体においてどのように出現しているか期間ごとの出現率の比較を行う．

5. 結果

第4章で示した手順に従い，2015年1月から2016年12月までに出現した検体の収集および解析を行った．

収集したマルウェアの種別の内訳は表1の通りである．

表 1　収集済み検体に関して

Table 1　List of collected specimens.

マルウェア種別	検体数
EMDIVI	77
PlugX	616
POISON	513
ChChes	24

収集を行った期間において，初期段階で行った短期間での発生パターン[26]と，期間を延長することで取得を行った長期間の発生パターンの 2 点に関して分析を行った．

5.1 従来の分析結果

2015 年 6 月から 9 月の期間に関して，機能を月毎の出現率として比較したものから明らかになった変化は以下の通りである．

A) 「EMDIVI」は「バックドア」として検知される比率が増大の傾向にあり，今後も同様であると考えられる．

B) 「EMDIVI」は「C&Cサーバとのトラフィック」，「到達不能なHTTPリンクへリクエスト」に関して，共に減少する傾向があり，今後も同様であると考えられる．

C) 動作環境を検索する機能である「実行プロセスの列挙」，「ユーザアカウント名の取得」の2つの項目において，「EMDIVI」では先行する2種のマルウェアに追随する形で増加しており，今後も同様であると考えられる．

5.2 分析期間の延長

分析期間を収集が完了している 2015 年 1 月から 2016 年 12 月まで延長することでより長期的な発生パターンの調査を行うことができた．機能に関して，半期ごとの出現率の比較したものが表 2 である．以降，比較した結果から明らかになったものについて述べていく．

5.2.1 従来の分析結果との比較

A) 「EMDIVI」および「ChCes」におけるシグニチャによる検知内容としては，「バックドア」とする比率よりも「トロイの木馬」とするものが多くを占めている．

B) 「EMDIVI」における「C&C サーバとのトラフィック」は従来の分析結果と同様に減少傾向にあることが確認できた．「到達不能な HTTP リンクへリクエスト」に関して，2016 年の上半期までは減少傾向にあったものの，2016 年の下半期には再び出現している機能となっている．また，類似性のある「ChChes」に関しても「C&C サーバとのトラフィック」は確認することが出来なかった．

C) 「EMDIVI」における実行プロセスの列挙」，「ユーザアカウント名の取得」に関しては継続して増加の傾向を確認することができた．しかし，従来の結果から述べられていた「POISON」「PlugX」に追随する形という部分は確認できなかった．また，類似性のある「ChChes」に関しても同様の機能を確認することができた．

5.2.2 新たな変化

A) 「PlugX」において，解析を回避するための「解析環境の失速（スリープ）」の機能に関して，出現率が対象期間内で 0.0%から 54.7%まで増加していることが確認できる．このことから「PlugX」を用いる攻撃者の中で解析を回避する機能を備えさせる傾向にあることが長期の変化から考えられる．

B) 「POISON」において，「潜在的な悪意のあるアプリケーション/プログラム（metasploit）」に属するという解析結果が 2016 年に入り，56.7%から 70.0%と増加していることが確認できる．

「POISON」は今回対象としている他の検体よりも先行して出現している種別なので，今後同様の機能が他の種別においても登場するということが考えられる．

C) 「EMDIVI」において，「他のプロセスのメモリをデバッグまたは読み取る権限を与える（SeDebugPrivilege）」の機能に関して，出現率が対象期間内で 27.8%から 50.0%まで増加していることが確認できる．同様の機能が「ChChes」においても確認できる．「EMDIVI」

に類似する種別としてされることから，今後「ChChes」においても同様の機能が多く確認できるのではないかと考える．

6. 考察

第 5 章より ，各マルウェアの機能がどのように変化するかを明らかにすることで，事前の予測に対しての比較における検証するとともに，より多くの期間を対象とした発生パターンの調査を行うことで，以下のような発生パターンを明らかにすることができた．

A) 「EMDIVI」において，「C&C サーバとのトラフィック」が減少傾向にあることが従来の結果と合わせて明らかになった．また，類似性の種別である「ChChes」に関しても「C&C サーバとのトラフィック」は確認することが出来なかった．

B) 「EMDIVI」において，「実行プロセスの列挙」，「ユーザアカウント名の取得」が増加傾向にあることが従来の結果と合わせて明らかになった．また，類似性のある「ChChes」に関しても同様の機能を確認した．

しかし，従来の結果で述べられていた「POISON」「PlugX」に追随する形という部分は確認できなかった．

C) 「PlugX」において，解析を回避するための「解析環境の失速（スリープ）」の機能が増加傾向にあることが長期の変化から明らかになった．

D) 「POISON」において，「潜在的な悪意のあるアプリケーション/プログラム（metasploit）」の機能 2016 年に入り，増加傾向にあることを明らかにし，後続である他の種別においても同様の機能が登場するという予測を行った．

E) 「EMDIVI」において，「他のプロセスのメモリをデバッグまたは読み取る権限を与える（SeDebugPrivilege）」の機能に関して，増加傾向にあることが長期の変化から明らかになった．また，類似性のある「ChChes」においても同様の機能が確認でき，増加するのではないかという予測を行った．

本研究で収集および動的な解析を行った検体の中にはシグネチャによる検知結果のみの検体が存在した．この解析結果が，検体に機能が存在しないことによるものであるか，マルウェアが持つ耐解析機能により Lastline 上で動作を行わなかったためであるか，更なる調査の必要があると考える．

表 2　機能の出現率

Table 2　Percentage of occurrence of function.

		2015年						2016年						
		上半期			下半期			上半期			下半期			
		EMDIVI	PlugX	POISON	EMDIVI	PlugX	POISON	EMDIVI	PlugX	POISON	EMDIVI	PlugX	POISON	ChChes
自動実行	ログオンプロセスを自動起動に変更	72.2%	0.0%	0.0%	16.7%	1.4%	0.0%	42.9%	0.0%	20.0%	40.0%	0.0%	3.3%	0.0%
	起動時に新しいサービスを登録	0.0%	41.2%	0.0%	0.0%	58.6%	0.0%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	0.0%
	Windowsの起動時に自動起動を登録	5.6%	41.2%	0.0%	0.0%	17.1%	0.0%	0.0%	14.3%	10.0%	30.0%	78.3%	3.3%	29.2%
	Windowsのスタートメニューを使用して自動起動を登録	11.1%	0.0%	50.0%	40.5%	2.9%	16.4%	0.0%	0.0%	23.3%	30.0%	0.0%	3.3%	0.0%
回避	マウスの動作をチェックしてサンドボックスを検出する機能	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	76.4%	0.0%	0.0%
	現在のメモリの可用性を取得する機能	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	28.6%	16.7%	50.0%	0.9%	3.3%	0.0%
	特定の画像ファイル名を確認	5.6%	0.0%	50.0%	0.0%	0.0%	1.5%	0.0%	0.0%	3.3%	0.0%	0.0%	0.0%	0.0%
	解析環境の失速（スリープ）	0.0%	0.0%	0.0%	0.0%	7.1%	0.0%	0.0%	14.3%	0.0%	0.0%	54.7%	0.0%	4.2%
	特定のプロセスを検索する：explorer.exe（システムインジェクションのターゲット）	5.6%	0.0%	0.0%	9.5%	0.0%	22.4%	0.0%	0.0%	0.0%	50.0%	0.0%	0.0%	0.0%
実行	異常な引数を持つコマンドラインシェルを実行	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	76.4%	0.0%	0.0%
ファミリ	リモートでディレクトリを参照する機能	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	76.4%	0.0%	0.0%
	リモートでコマンドを渡す機能	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	76.4%	0.0%	0.0%
	潜在的な悪意のあるアプリケーション/プログラム（metasploit）	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	56.7%	0.0%	0.0%	70.0%	0.0%
ファイル	Windowsディレクトリで実行可能ファイルを変更	0.0%	5.9%	50.0%	0.0%	7.1%	9.0%	0.0%	0.0%	3.3%	0.0%	0.0%	0.0%	0.0%
	ユーザー共有データディレクトリでの実行可能ファイルの変更	0.0%	35.3%	0.0%	0.0%	62.9%	0.0%	0.0%	0.0%	0.0%	0.0%	1.9%	0.0%	0.0%
メモリ	プロセスのイメージを同じオリジナルの実行可能ファイルに置き換える（潜在的なアンパック）	0.0%	0.0%	0.0%	0.0%	1.4%	1.5%	0.0%	0.0%	10.0%	0.0%	0.9%	3.3%	0.0%
	別のプロセスのイメージの置き換え（検出の回避または特権の昇格）	0.0%	88.2%	0.0%	0.0%	71.4%	28.4%	0.0%	0.0%	6.7%	0.0%	3.8%	0.0%	4.2%
	実行中の子でないプロセスのメモリへの書き込み	0.0%	35.3%	0.0%	0.0%	45.7%	23.9%	0.0%	0.0%	3.3%	0.0%	0.0%	0.0%	0.0%
ネットワーク	インターネットからファイルをダウンロードする機能	5.6%	0.0%	0.0%	2.4%	1.4%	0.0%	0.0%	0.0%	0.0%	50.0%	0.9%	0.0%	0.0%
	コードインジェクションによるネットワークアクティビティの非表示	0.0%	88.2%	0.0%	0.0%	65.7%	0.0%	0.0%	0.0%	0.0%	0.0%	3.8%	0.0%	4.2%
	C&Cサーバとのトラフィックの確認	27.8%	5.9%	0.0%	28.6%	10.0%	0.0%	14.3%	14.3%	0.0%	0.0%	0.9%	0.0%	0.0%
	ダイナミックDNSドメインに接続	0.0%	0.0%	50.0%	0.0%	1.4%	14.9%	0.0%	0.0%	13.3%	0.0%	0.0%	0.0%	0.0%
	ハードコードされたプライベートIPアドレスに接続	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	14.3%	36.7%	0.0%	0.0%	60.0%	0.0%
	ハードコードされたIPアドレスを使用してサーバーに接続	0.0%	11.8%	0.0%	0.0%	20.0%	4.5%	0.0%	14.3%	16.7%	0.0%	52.8%	16.7%	0.0%
	シンクホールドメインへの接続	0.0%	0.0%	0.0%	0.0%	1.4%	0.0%	28.6%	0.0%	0.0%	20.0%	25.5%	0.0%	0.0%
	サーバーとの通信に失敗	0.0%	35.3%	0.0%	0.0%	35.7%	16.4%	0.0%	0.0%	20.0%	0.0%	50.9%	16.7%	0.0%
	到達不能なHTTPリンクを要求	72.2%	5.9%	0.0%	38.1%	4.3%	0.0%	14.3%	0.0%	0.0%	70.0%	0.9%	0.0%	0.0%
パッカー	埋め込まれたPEイメージの読み込み（潜在的なアンパック）	0.0%	0.0%	0.0%	0.0%	10.0%	9.0%	0.0%	14.3%	10.0%	0.0%	0.0%	3.3%	0.0%
検索	ユーザーアカウント名の取得	5.6%	76.5%	0.0%	14.3%	50.0%	0.0%	0.0%	0.0%	0.0%	30.0%	78.3%	0.0%	4.2%
	実行中のプロセスを列挙	5.6%	17.6%	0.0%	11.9%	55.7%	0.0%	0.0%	14.3%	3.3%	50.0%	1.9%	0.0%	4.2%
設定	他のプロセスのメモリをデバッグまたは読み取る権限を与える（SeDebugPrivilege）	27.8%	0.0%	0.0%	28.6%	4.3%	0.0%	42.9%	0.0%	20.0%	50.0%	0.9%	3.3%	4.2%
シグネチャ	バックドアのコードとして識別	11.1%	5.9%	100.0%	42.9%	1.4%	68.7%	28.6%	0.0%	76.7%	40.0%	0.0%	100.0%	12.5%
	トロイの木馬のコードとして識別	77.8%	94.1%	0.0%	52.4%	98.6%	31.3%	57.1%	57.1%	20.0%	60.0%	83.0%	0.0%	83.3%
窃取	ウィンドウフックを設定する機能（WH_KEYBOAR	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	28.6%	0.0%	0.0%	0.9%	3.3%	0.0%
	キーストロークロギング機能	0.0%	76.5%	0.0%	0.0%	57.1%	10.4%	0.0%	0.0%	10.4%	0.0%	0.0%	0.0%	0.0%
ステルス	システムファイルになりすます実行ファイルの作成	0.0%	35.3%	0.0%	0.0%	1.4%	6.0%	0.0%	14.3%	0.0%	0.0%	0.0%	0.0%	0.0%
	隠された実行可能ファイルの作成	0.0%	35.3%	0.0%	0.0%	58.6%	9.0%	0.0%	0.0%	6.7%	0.0%	4.7%	3.3%	0.0%
	実行後のサンプルの削除	0.0%	35.3%	0.0%	0.0%	4.3%	0.0%	0.0%	0.0%	0.0%	0.0%	76.4%	0.0%	0.0%

7. おわりに

本研究では，実際の標的型攻撃の際に使用されたマルウェアである「EMDIVI」,「PlugX」,「POISONIVY」,「ChChes」の4種に対して，約2年間という期間を対象として解析・比較を行った．その結果，長期間に渡ってマルウェア機能の変化を明らかにすることでき，新たに発生パターンを得ることができた．加えて，従来の分析により求めていた発生パターンの検証を行うことで発生パターンにより説得力を持たせることができた．

現状では，特定期間の傾向の導出にとどまっているが，対象とする期間を延ばすことで，現在調査可能なすべての期間においての検証，分析を引き続き行っていく．そのために今後は,データ量増加に向けて第4章で述べたプロセスの自動化の検討を行っている．自動化を実現することにより,より多くのデータの収集を効率的に行えるだけでなく，情報の共有や分析に対しても様々なアプローチが行えるようになると考えている．

そのほか，マルウェアの機能に何か大きな変化が起きた際に，その背景に社会的な事象があるか調査を行うことで機能の予測に有用な情報になると考えている．そうした場合，現在取得している発生パターンにおいても更なる検証を行うことが必要であると考える．

謝辞　本研究に際して,様々なご指導を頂きました LIFT プロジェクトの関係者に深謝いたします.

参考文献

[1] Symantec : 「標的型攻撃」に備えるサイバー攻撃 : 標的型攻撃とは，APT とは，Symantec（オンライン），入手先 <http://www.symantec.com/ja/jp/theme.jsp?themeid=apt_insight>.
[2] f5 : 標的型攻撃, f5(オンライン), 入手先 <https://f5.com/glossary/glossary135-21618>.
[3] Canon : 従来型セキュリティ対策の限界を超える, 次世代セキュリティのアプローチとは, Canon(オンライン), 入手先 <https://eset-info.canon-its.jp/malware_info/special/detail/150312.html>.
[4] 情報処理推進機構 : 脆弱性を利用した新たなる脅威の監視・分析による調査 (online), 入手先 <https://www.ipa.go.jp/files/000017745.pdf>.
[5] Symantec : アンダーグラウンドのブラックマーケット : 盗難データ，マルウェア，攻撃サービスの取引が盛況, Symantec(オンライン), 入手先 <http://www.symantec.com/connect/ja/blogs-367>.
[6]G DATA : G DATA SECURITYLABS MALWARE REPORT,G DATA (online), available from <https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H2_2014_EN_v1.pdf >.
[7]Canon : ヒューリスティック「基礎編」未知のウイルスも検出して駆除する ESET のヒューリスティック機能, Canon(オンライン), 入手先 <http://canon-its.jp/eset/malware_info/technology/140626/>.
[8] 佐々木良一, 上原哲太郎, 松本隆 : 標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望, 情報処理学会コンピュータセキュリティシンポジウム 2013(CSS2013), pp.155-162.
[9] 比留間裕幸, 橋本一紀, 柿崎淑郎, 八槇博史, 上原哲太郎, 佳山こうせつ, 松本隆, 佐々木良一 : 標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発(その１）－予兆検知と対策方法の提案－, マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015), pp.29-37.
[10] 橋本一紀, 比留間裕幸, 上原哲太郎, 松本隆, 佳山こうせつ, 柿崎淑郎, 八槇博史, 佐々木良一 : 標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発(その２）－プロトプログラムの開発と評価－, マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015), pp.38-43.
[11] 佐々木良一, 八槙博史 : 標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発（その 3）－今後の研究構想－, マルチメディア，分散，協調とモバイルシンポジウム 2015(DICOMO2015), pp.44-50.
[12] ZDNet Japan : JTB，793 万人分の個人情報流出か--外部への通信で不正アクセスと判明, ZDNet Japan(オンライン), 入手先 <https://japan.zdnet.com/article/35084254/>.
[13] VirusTotal : https://www.virustotal.com/
[14] Lastline Analyst : https://www.lastline.com/platform/analyst
[15] 堀合 啓一, 今泉 隆文, 田中 英彦 : マルウェア亜種の動的挙動を利用した自動分類手法の提案と実装, 情報処理学会論文誌, vol.50, no.4, pp.1321-1333.
[16] 畑田 充弘, 森 達哉 : 実行時の通信挙動を用いたマルウェアの分類と未知検体検出への応用,CSS2016 論文集, vol.2016, pp.647-654.
[17] 鈴木 文仁, 上原 哲太郎, 名和 利夫, 佳山 こうせつ, 村上弘和, 堀添裕太, 佐々木良一 : 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 1）－LIFT の全体像－, 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017).
[18] 島崎一樹, 勅使河原可海, 柿崎淑郎, 佐々木良一 : 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 2）－対策案優先度評価法－, 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017).
[19] 島川貴裕, 佐藤信, 佐々木良一 : 標的型に対する知的ネットワークフォレンジックシステム LIFT の機能拡張（その 3）－侵入源と波及範囲の推定－, 情報処理学会コンピュータセキュリティシンポジウム 2017(CSS2017).
[20] 石川 博也, 八槇 博史 : サイバー空間における攻撃と防御の共進化シミュレーション, CSS2016 論文集, vol.2016, pp.1341-1348.
[21] TREND MICRO : 国内標的型サイバー攻撃分析レポート 2015 年版 -「気付けない攻撃」の高度化が進む, TREND MICRO(オンライン), 入手先 <https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161>.
[22] TREND MICRO : 国内標的型サイバー攻撃分析レポート 2016 年版 - 状況と目的に応じて攻撃を変化させる攻撃者, TREND MICRO(オンライン), 入手先 <https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=194>.
[23] TREND MICRO : 国内標的型サイバー攻撃分析レポート 2017 年版 -巧妙化と高度化を続ける「気づけない」攻撃, TREND MICRO(オンライン), 入手先 <https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=225>
[24] ZDNet Japan : 年金機構事件で発覚--感染に気付かれず潜伏する「Emdivi」の恐ろしさ, ZDNet Japan(オンライン), 入手先 <http://japan.zdnet.com/article/35065996/>.
[25] Malwr - Malware Analysis by Cuckoo Sandbox: https://malwr.com/
[26] 渋谷健太, 久山真宏, 佐藤信, 三村聡志, 松本隆, 佐々木良一 : 標的型攻撃に対する知的ネットワークフォレンジックシステム LIFT の開発－標的型攻撃マルウェアの解析と亜種の予測－, マルチメディア，分散，協調とモバイルシンポジウム 2016(DICOMO2016), pp.1081-1086 .