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 －模擬 C&C サーバを用いたマルウェアの挙動解析－

島川貴裕[1] 久山真宏[1] 佐藤信[1] 名和利男[1] 高倉弘喜[1] 佐々木良一[1]

概要： 近年，特定の組織や個人を攻撃対象とする標的型攻撃が社会的な問題となっている．標的型攻撃は，非常に巧妙な攻撃であり，攻撃の痕跡を発見することが難しいうえに，適切な対応が難しい現状がある．そこで，著者らは，標的型攻撃に対応するために LIFT（Live and Intelligent Network Forensic Technologies）システムおよび Super-LIFT システムの開発を行っている．Super-LIFT システムを実現するためには，日々巧妙化する攻撃に関する情報を収集する必要がある．しかし，攻撃を発見した時には，感染端末などから攻撃の痕跡の多くが消去されていることや，攻撃に利用された C&C サーバの停止により攻撃に関する情報を十分に収集できていない現状がある．そこで本稿では，C&C サーバと連携するマルウェアの挙動に着目し，C&C サーバへの模擬通信とマルウェアの動的解析の繰り返しにより C&C サーバと連携するマルウェアの挙動の解析を行うための手法を提案する．今回の実験結果から，C&C サーバと連携するマルウェアの挙動の一端として攻撃基盤の構築段階の挙動を確認できた．そのため，本提案手法により，標的型攻撃の一連の流れを把握し，従来マルウェアだけの挙動から推測する必要のあった標的型攻撃そのものの情報をより詳細に収集可能となると考える．さらに，LIFT システムおよび Super-LIFT システムがこの機能を利用することで今後出現すると考えられる新しい攻撃にも対応可能になると考える．

Development of intellectual network forensic system LIFT against targeted attack －Analysis of malware using dummy C&C Servers－

TAKAHIRO SHIMAKAWA[1] MASAHIRO KUYAMA[1] MAKOTO SATO[1]
TOSHIO NAWA[1] HIROKI TAKAKURA[1] RYOICHI SASAKI[1]

1. はじめに

近年，特定の組織や個人を攻撃対象とし情報窃取を行う標的型攻撃が社会的な問題となっている．日本では，2011 年 9 月には三菱重工，2013 年 1 月には農林水産省などが被害に遭っており，2015 年 6 月には日本年金機構が被害に遭い 125 万件の個人情報が流出した[1].

標的型攻撃は，さまざまな攻撃手法を巧みに組み合わせて攻撃を行う．攻撃に用いられるマルウェアには，感染を容易にするために実装する機能を限っているという特徴がある[2]．そのため，マルウェアに感染したコンピュータに指令を送信し，動作を制御するために用いられる C&C（Command and Control）サーバ[3]と連携して，攻撃に必要とするツールなどをダウンロードしながら攻撃を遂行していく非常に巧妙な攻撃であり，攻撃の痕跡を見つけるのが難しい．

標的型攻撃に対応するために，2013 年に LIFT プロジェクトを立ち上げ，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攻撃の影響を軽減するための応急対応を支援する LIFT システムの開発を行っている[4]．LIFT プロジェクトをさらに発展させ，今後出現すると考えられる新しい攻撃にも対応することを目的とする Super-LIFT システムの構想にも着手している[5]．Super-LIFT システムを実現するためには，日々巧妙化する攻撃に関する情報を収集する必要がある．しかし，攻撃を発見した時には，感染端末などから攻撃の痕跡の多くが消去されていることや，C&C サーバが停止しているなど攻撃に関する情報の収集が十分にできないといった問題がある．

そこで，本研究では，LIFT システムおよび Super-LIFT システムの研究の一環として，マルウェアと C&C サーバの連携に着目し，C&C サーバと連携するマルウェアの挙動の解析を行うための手法を提案する．これにより，標的型攻撃の一連の流れを把握し，従来マルウェアだけの挙動から推測する必要のあった標的型攻撃そのもの情報をより詳細に収集可能とした．さらに，LIFT システムおよび Super-LIFT システムがこの機能を利用することで今後出現すると考えられる新しい攻撃にも対応可能になると考える．

まず，第 2 章で先行研究，第 3 章で関連研究について述

1 東京電機大学
Tokyo Denki University

べ，第 4 章で C&C サーバと連携するマルウェアの挙動の解析を行うための手法を提案する．第 5 章で提案手法による実験とその結果について述べ，第 6 章で考察を行う．そして最後に第 7 章で今後の展望を含めたまとめを述べる．

2. 先行研究

2.1 LIFT システム

LIFT 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て攻撃の推定，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り，当研究室で開発を進めている[4]．図 1 に LIFT システムの機能概略を示す．LIFT システムでは，まず各ネットワーク機器や端末，検知ツールから攻撃事象における徴候を収集する．収集した徴候から徴候・事象関連テーブル（徴候と事象の関連を定義したテーブル）を用いて攻撃事象を確定し，事象・対策関連テーブル（事象と対策の関連を定義したテーブル）を用いて有効な対策案の算出を行い，運用者へガイドラインを表示する．これにより，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攻撃の影響を軽減するために適切な応急対応が行えるよう支援する．

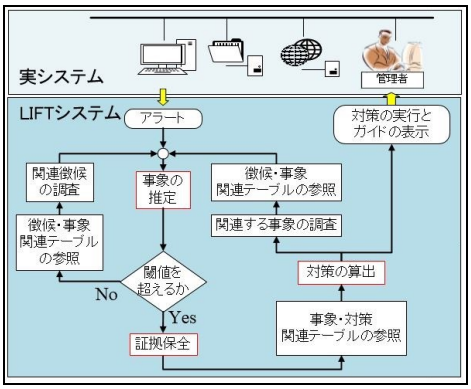

図 1　LIFT システムの機能概略

2.2 Super-LIFT システム

Super-LIFT システムとは，LIFT システムを拡張し既存の攻撃だけではなく，今後出現すると考えられる新しい攻撃のパターンを予測し，シミュレーションすることにより先回りした対策の実現を可能とすることを目的としたシステムであり，当研究室で開発を進めている[5]．図 2 に Super-LIFT システムの機能概要を示す．Super-LIFT システムは，AI 利用攻撃ケース自動生成サブシステムと対応ルール自動生成サブシステムの二つのサブシステムから構成される．

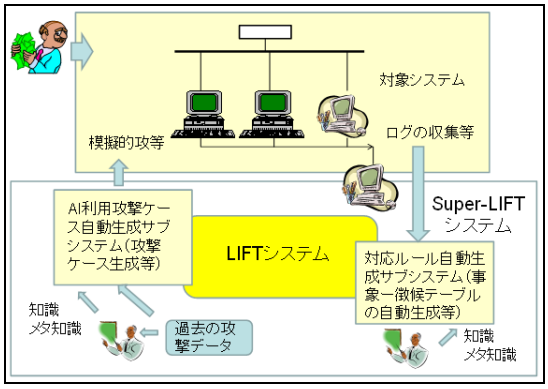

図 2　Super-LIFT システムの機能概要

2.2.1 AI 利用攻撃ケース自動生成サブシステム

図 3 に AI 利用攻撃ケース自動生成サブシステムの概要を示す．AI 利用攻撃ケース自動生成サブシステムでは，外部から収集した攻撃データを基に攻撃ケースの生成を行う．

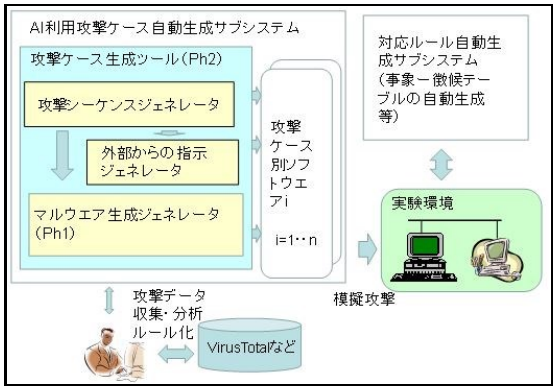

図 3　AI 利用攻撃ケース自動生成サブシステム

2.2.2 対応ルール自動生成サブシステム

図 4 に対応ルール自動生成サブシステムの概要を示す．対応ルール自動生成サブシステムでは，AI 利用攻撃ケース自動生成サブシステムにより生成された攻撃ケースによる模擬攻撃の結果を基に攻撃に対応したルールの自動生成を行う．

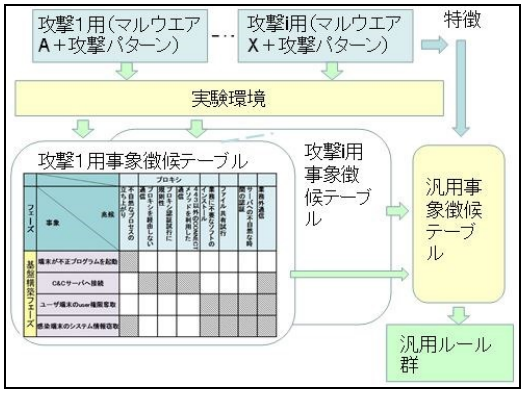

図 4　対応ルール自動生成サブシステム

これらのサブシステムにより,既存の攻撃だけではなく,今後出現すると考えられる新しい攻撃であっても先回りした対策の実現を可能とする.

本研究は,LIFT システムにおける徴候・事象関連テーブルの正確性の向上および Super-LIFT システムにおける模擬攻撃の生成を行うために必要となる攻撃データの収集・分析に位置づけられる.

3. 関連研究

マルウェアの解析手法は大きく分けて静的解析と動的解析の二つに分けられる.

静的解析とは,マルウェアの実行ファイルを逆アセンブルし,得られたアセンブリコードからマルウェアの機能や構造の解析を行う手法である[6].しかし,近年のマルウェアには,実行形式を保ったまま圧縮・難読化を施すパックという技術が使用されている[7].そのため,静的解析では,まずパックを解除する必要がある.

一方,動的解析とは,マルウェアを解析環境内で実際に動作させ,その挙動を観測することにより解析を行う手法である[6].そのため,パックの影響を受けないという利点がある.また,動的解析は,一定時間マルウェアを実行させる解析手法であるため静的解析に比べて解析にかかる時間を短くすることができる[6].そのため,増加傾向にあるマルウェアに対して有効な解析手法といえる.しかし,動的解析では,マルウェアが動作する環境を整える必要がある.そこで,文献[8]では,マルウェアの実行環境や実行方法を工夫することによって解析の精度を向上する検討が行われている.本研究ではマルウェアの実行環境として実際の被害環境に近づけた環境を構築し解析を行っていくことで解析の精度の向上を図った.

標的型攻撃に用いられるマルウェアのような外部と連携するマルウェアの場合,解析環境を外部との通信を許可するなどして動的解析を行わなければマルウェアの本来の挙動を観測することができない.しかし,解析環境が外部との通信を許可する場合,外部に攻撃を行うリスクが発生する.文献[9,10]では,マルウェアの通信をその内容に応じてネットワーク接続制御を行い危険性が低いと判断したもののみ外部との通信を許可するマルウェア動的解析システムを提案している.

本研究では,マルウェアを動作させる環境は外部との通信を許可せず,マルウェアが行った通信をマルウェアが感染していない別環境下で通信のみを模擬する手法をとる.このような手法をとって解析を行っている研究に文献[11]がある.文献[11]では,マルウェアが C&C サーバへ行う同一の通信であっても C&C サーバの応答が時期によって変化することに着目し,その応答を収集し収集した応答を用いて時期によって異なるマルウェアの挙動の解析を行っている.しかし,本研究で解析対象とする標的型攻撃に用いられるマルウェアの場合,通信を行う C&C サーバは攻撃者が解析を妨害するために停止させることが多く時期によって変化するとは考えにくい.また,文献[11]では,C&C サーバからの応答を収集後の動的解析を一回だけ行っていたが,標的型攻撃に用いられるマルウェアは C&C サーバへの通信は一回だけではなく複数回行われるため,C&C サーバからの応答の収集と動的解析を繰り返し行わなければ,十分な解析結果を得られないと考える.そこで,本研究では,通信の模擬による情報の収集と動的解析を繰り返し行うことで標的型攻撃に用いられるマルウェアの挙動の解析を行う.

4. 提案手法

提案する C&C サーバと連携するマルウェアの挙動の解析手法は以下の解析手順を踏む.

1. 事前準備
2. 模擬通信
3. 動的解析
4. 2 と 3 の繰り返し

4.1 事前準備

事前準備では,サンドボックス(不審なプログラムを隔離された環境上で実行するためのセキュリティ機構[12])によるマルウェアの動的解析を行い,マルウェアが C&C サーバへ送信するリクエストを取得し,通信エラーの出ていないマルウェアの抽出を行う.これにより,未だ稼動している可能性のある C&C サーバの抽出を行う.本研究では,pcap ファイルでマルウェアが行った通信ログを取得することができる動的解析サービスである Lastline Analyst[13]を使用した.

4.2 模擬通信

模擬通信では,事前準備により抽出したマルウェアが,C&C サーバへ送信するリクエストを基に,実際に C&C サーバと通信を行い,通信により取得されるファイルの収集を行う.具体的には,マルウェアに感染していない環境下で通信先の URL をマルウェアが送信したものに変更し C&C サーバと通信を行う.そのために,ローカルプロキシを使用しリクエストを一旦キャプチャし,C&C サーバへ送信するリクエストをマルウェアが送信したものに変更する.これにより,C&C サーバとの通信により取得されるファイルの収集を行う.また,本研究ではローカルプロキシツールである BurpSuite[14]のプロキシ機能を使用した.

4.3 動的解析

動的解析では,サンドボックスによる解析が行える範囲

外の解析を行う．そのために，マルウェアに模擬通信により取得したファイルを与え，ファイル取得後の挙動の解析を行う．

4.4 模擬通信と動的解析の繰り返し

動的解析の結果，新たな通信が発生した場合，より詳細な解析を行える可能性がある．そのため，再度模擬通信を行い，解析環境のチューニングが必要な場合チューニングを行い，再度動的解析を行う．このように模擬通信と動的解析の二つの作業を繰り返し行うことで C&C サーバと連携したマルウェアの挙動の解析を行う．本提案手法による解析を行うことで C&C サーバと連携するマルウェアの挙動の解析を行うことができ，標的型攻撃そのものの情報をより詳細に収集することが可能であると考える．

5. 実験

5.1 概要

実験では，2014 年の標的型攻撃に使用されたマルウェアの中で使用率の高い上位 3 種のマルウェア（EMDIVI，PLUGX，POISONIVY）[15]について提案手法による解析を行った．

解析時間については文献[16]を参考にした．文献[16]では，100 秒から 120 秒程度を解析時間と設定すれば，1800 秒間で実行される約 90%の挙動の解析結果を得られるという結果を得ている．そのため，今回の実験では動的解析の解析時間を 120 秒とした．

5.2 解析環境

解析環境のネットワーク図を図 6 に示す．本環境のネットワークは LAN，DMZ，擬似インターネットの 3 つのセグメントから構成される．また，解析環境内の各マシンの構成を表 1 に示す．今回の実験では，全て仮想環境内に構築した．

5.2.1 LAN

Active Directory（管理するネットワーク上のユーザ情報などを一元管理するしくみ[17]）は，解析環境をより実環境に近づけるために構築し，解析 PC とファイルサーバの登録を行った．さらに，同一マシン上に DHCP サーバを構築し，解析 PC に IP アドレスを自動的に発行するようにした．

解析 PC はマルウェアを実行し，その挙動の監視を行うための被害 PC である．また，マルウェアの監視には，プロセスが行った処理をリアルタイムで表示・記録するツールである Process Monitor[18]とパケットキャプチャツールである Wireshark[19]を使用した．

ファイルサーバは，Active Directory 同様に解析環境をより実環境に近づけるために構築した．

5.2.2 DMZ

DNS サーバには，DNS の応答を偽装するツールである ApateDNS[20]を使用した．これにより，解析 PC 内で実行したマルウェアからの通信が模擬 C&C サーバに転送されるようにした．

プロキシサーバは，Active Directory 同様に解析環境をより実環境に近づけるために構築した．

5.2.3 擬似インターネット

模擬 C&C サーバは，実インターネット上のサーバ群を模倣し，マルウェアに対してネットワークサービスを提供すると共に，マルウェアから要求のあったファイルを返信するために構築した．実インターネットの模倣では，FTP サーバ，NTP サーバ，IRC サーバ，SMTP サーバ，HTTP サーバといった一般的に利用可能なサービスを模倣する．これらのサーバ群は各サービスをデフォルトポートにおいて提供する．また，サービスを用意していないポートに対しては受信したデータをそのまま返答する ECHO サーバが応答するようにした．

5.2.4 ルータ

ルータは，firewalld により構築し DNS サーバおよびプロキシサーバで使用するポート以外は擬似インターネットへ転送するように設定した．

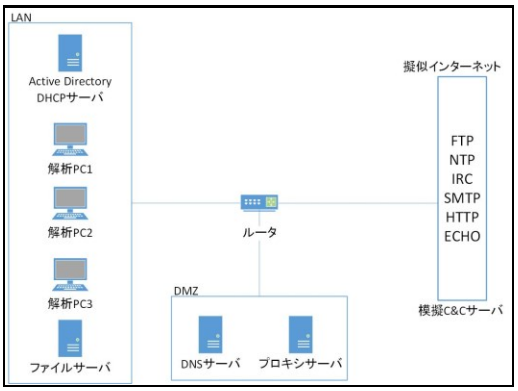

図 6　解析環境のネットワーク図

表 1　解析環境内の各マシンの構成

セグメント	用途	OS
LAN	Active Directory DHCP サーバ	Windows Server 2012
	解析 PC	Windows XP SP3
	ファイルサーバ	Windows Server 2012
DMZ	DNS サーバ	Windows 7
	プロキシサーバ	CentOS7
擬似インターネット	模擬 C&C サーバ	CentOS7
	ルータ	CentOS7

5.3 事前準備の結果

事前準備による解析の結果，通信エラーの出ていなかった検体数を表 2 に示す.

表 2　通信エラーの出ていなかった検体数の割合

種別	検体数
EMDIVI	16/70
PLUGX	30/115
POISONIVY	24/72

通信エラーの出ていなかった検体数は，EMDIVI では 16 検体，PLUGX では 30 検体，POISONIVY では 24 検体であった．これらの検体が通信を行った C&C サーバは未だ稼動している可能性があるため模擬通信を行い，通信により取得されるファイルの収集を行った.

5.4 模擬通信の結果

未だ C&C サーバが稼動している可能性がある表 2 の検体において模擬通信を行った結果，通信が成功した検体数を表 3 に示す.

表 3　通信が成功した検体数

種別	検体数
EMDIVI	5/16
PLUGX	11/30
POISONIVY	2/24

通信が成功した検体数は，EMDIVI では 5 検体，PLUGX では 11 検体，POISONIVY では 2 検体であった.

しかし，EMDIVI の 5 検体のうち 4 検体は大手検索サイトのトップページへのアクセスであった．そのため，この通信はマルウェアが感染端末がネットワークに繋がるかを確認するための通信であると判断した．また，PLUGX の 11 検体のうち 4 検体は，通信は成功したがファイルを取得することができなかった．そのうち 2 検体は，シンクホール（マルウェアからの通信を観測するために研究機関が用意したサーバ[21]）への通信であった．そのため，これらの通信は C&C サーバとの通信ではないと判断した．結果として模擬通信により C&C サーバと通信しファイルを取得できた検体数は表 4 に示す通りである.

表 4　C&C サーバと通信しファイルを取得できた検体数の割合と取得したファイル

種別	検体数	ファイル
EMDIVI	1/5	zip
PLUGX	7/11	txt，cab，crl
POISONIVY	2/2	exe

C&C サーバと通信しファイルを取得できた検体数は，EMDIVI では 1 検体で zip ファイルを取得でき，PLUGX では 7 検体で txt ファイル，cab ファイル，crl ファイルを取得でき，POISONIVY では 2 検体で exe ファイルを取得できた．これらの検体は，収集したファイルを与え，ファイル取得後の挙動を誘発させることでサンドボックスによる解析が行える範囲外の解析を行える可能性があるため動的解析を行った.

5.5 動的解析の結果

5.5.1 EMIDVI

マルウェアの実行を開始すると pdf ファイルを開く処理が行われたが，解析 PC 内に pdf ファイルを開くためのソフトウェアが無かったため開くことができなかった．そのため，pdf ファイルが正常に開かれるようにするために Windows XP でも動作する Adobe Acrobat Reader を解析 PC にインストールし再度動的解析を行った．その結果，模擬通信で取得したファイルを取得する通信が行われたが，相対パスが違ったため通信エラーとなっていた．再度模擬通信を行ったが取得したファイルには，zip ファイル中のファイルで使用されている言語の違いしかなかった．模擬 C&C サーバ内に取得したファイルを配置し，再度動的解析を行った結果，通信が成功していた．また，取得したファイルに対してはマルウェアが起動させたプロセスが操作を行っていた.

5.5.2 PLUGX

マルウェアの実行を開始するとインストーラを子プロセスとして利用し，インストール処理が行われた．また，模擬通信で取得したファイルを取得する通信は解析時間内に確認できなかった．これらの挙動は 7 検体ともに共通していた.

5.5.3 POISONIVY

マルウェアの実行を開始するとトロイの木馬型のウィルスがデスクトップに隠しファイルとして作成された．また，模擬通信で取得したファイルを取得する通信を行っていたが，取得したファイルに対する操作は解析時間内に確認できなかった．これらの挙動は 2 検体ともに共通していた．

6. 考察

提案手法による解析を行った結果，マルウェアが必要としているファイルを与えることでファイル取得後の挙動を確認することができた．そのため，提案手法による解析により，C&C サーバと連携するマルウェアの挙動の解析を行うことができ，標的型攻撃そのものの情報をより詳細に収集することが可能であると考える．

今回の実験では，感染端末のファイルおよびレジストリキーの作成・変更など主に感染端末に対する操作が確認された．そのため，標的型攻撃における攻撃基盤の構築段階までを観測できたが，マルウェアの動作条件をより考慮した解析を行うことで観測できると考える．例えば，今回の実験では，マルウェアが起動させたプロセスが解析時間内に処理を終了していなかったものが多かったため，解析時間を長くすることにより，より詳細な挙動と新たな通信を得られる可能性があると考える．

7. おわりに

本研究では，C&C サーバとの模擬通信とマルウェアの動的解析を繰り返し行うことで C&C サーバと連携するマルウェアの挙動の解析を行う手法を提案した．また，提案手法による解析を行った結果，マルウェアが必要としているファイルを与えることで，ファイル取得後の挙動を確認することができた．これにより，標的型攻撃そのものの情報をより詳細に収集可能となると考える．さらに，LIFT システムおよび Super-LIFT システムがこの機能を利用することで今後出現すると考えられる新しい攻撃にも対応可能になると考える．

今後は，解析を行う検体数を増やすとともに，解析時間について検討し，より多くのマルウェアの解析を行う．これにより，標的型攻撃の一連の流れを把握し，従来マルウェアだけの挙動から推測する必要のあった標的型攻撃そのものの情報をより詳細に収集可能とする．

参考文献

[1] 株式会社ラック: 標的型攻撃 対策指南書, 株式会社ラック(オンライン)，入手先<http://www.lac.co.jp/anti-apt/guidebook/>.

[2] 特定非営利活動法人，日本セキュリティ監査協会，APT による攻撃対策と情報セキュリティ監査研究会: APT 対策入門，pp.38-39，(2012 年).

[3] IPA 独立行政法人情報処理推進機構: 「高度標的型攻撃」対策に向けたシステム設計ガイド，IPA 独立行政法人情報処理推進機構(オンライン)，入手先<https://www.ipa.go.jp/security/vuln/newattack.html>.

[4] 比留間裕幸，橋本一紀，柿崎淑郎ほか: 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－, DICOMO2015, pp.29-37(2015).

[5] 佐々木良一, 八槇博史: 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）－今後の構想－, DICOMO2015, pp.44-50(2015).

[6] 新井悠，岩村誠，川小谷裕平ほか: アナライジング・マルウェア　フリーツールを使った感染事案対処，pp.4-5,12-14，(2010 年).

[7] IPA 独立行政法人情報処理推進機構: 脆弱性を利用した新たなる脅威の監視・分析による調査報告書，IPA 独立行政法人情報処理推進機構(オンライン)，入手先<https://www.ipa.go.jp/security/vuln/report/newthreat200907.html>.

[8] 山口和晃，堀合啓一，田中英彦: マルウェア解析の効率化手法の検討，CSS2009, Vol.2009, No.11, pp.925-930(2009).

[9] 芝田文，吉岡克成，四方順司ほか: マルウェア動的解析のネットワーク接続制御を支援するユーザインタフェースの提案，CSEC2009，Vol.2009, No.20(2009-CSEC-44), pp.277-282(2009).

[10] 廣野壮志，大平健司，山口由紀子ほか: 擬似インターネットを用いたマルウェア動的解析のためのパケット転送制御方式の開発，信学技報，Vol.113，No.95，ICSS2013-12，pp.67-72(2013).

[11] 笠間貴弘，吉岡克成，松本勉ほか: 疑似クライアントを用いたサーバ応答蓄積型マルウェア動的解析システム，CSS2009，Vol.2009，No.11, pp.661-666(2009).

[12] 岩井博樹: 標的型攻撃セキュリティガイド，pp.69，(2013 年).

[13] Lastline Analyst: https://www.lastline.com/platform/analyst

[14] BurpSuite: https://portsigger.net/burp/

[15] TREND MICRO: 国内標的型攻撃サイバー攻撃分析レポート 2015 年版，TREND MICRO(オンライン), 入手先<https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=161>.

[16] 青木一史，川小谷裕平，岩村誠ほか: 動的解析における検体動作時間に関する検討, CSS2010, Vol.2010, No.9, pp.543-548(2010).

[17] Active Directory: https://technet.microsoft.com/ja-jp/windowsserver/bb466131.aspx

[18] Process Monitor: https://technet.microsoft.com/ja-jp/sysinternals/processmonitor.aspx

[19] WireShark: https://www.wireshark.org/download.html

[20] ApateDNS: http://www.aldeid.com/wiki/Mandiant-ApateDNS

[21] ITpro: 観測すればすべてが見えるー日本を狙う攻撃者の手口と実態－DNS シンクホールが明かす、日本を狙う標的型攻撃の実態，ITPro(オンライン)，入手先<http://itpro.nikkeibp.co.jp/atcl/column/15/101400241/101400002/?rt=nocnt>(参照 2015-11-21).