Vol.2014-CSEC-65 No.18
Vol.2014-IOT-25 No.18
2014/5/23

標的型攻撃のシナリオ再現環境の構築

津田 侑[1,a)]　神薗 雅紀[1,2]　遠峰 隆史[1]　安田 真悟[1]　三浦 良介[1]　宮地 利幸[1]　衛藤 将史[1]
井上 大介[1]　中尾 康二[1]

概要：特定組織に狙いを定めたサイバー攻撃，標的型攻撃が社会問題となっている．標的型攻撃にはいくつかのフェーズがあり，攻撃者は複数のツールを駆使して活動することが各種解析レポートで報告されている．解析レポートでは攻撃用ツールやマルウェアの解析結果が個々の事象としてまとめられており，そのつながりは解析者が想定したシナリオで補完されている．これは解析時に既に停止されている C&C サーバを含む攻撃者環境の特定や被害環境に残された痕跡の収集を解析者自身が十分に行えないためである．そこで本研究では，標的型攻撃における攻撃者の活動を正確に把握するために一連の攻撃シナリオを再現できる環境を構築する．シナリオ再現環境はネットワークで接続された被害環境と攻撃環境，解析支援環境で構成される．被害環境には一般的な企業組織を想定した環境を構築し，攻撃環境には模擬 C&C サーバを実装する．解析支援環境には，被害環境・攻撃環境を柔軟に構築し，反復してシナリオを再現しやすくするために用いる．本稿の最後では標的型攻撃のシナリオの一例を実施することで被害環境に残された痕跡を洗い出し，本環境について考察する．

Implementation of an Environment for Reproducing Targeted Attacks

Yu Tsuda[1,a)]　Masaki Kamizono[1,2]　Takashi Tomine[1]　Shingo Yasuda[1]　Ryosuke Miura[1]
Toshiyuki Miyachi[1]　Masashi Eto[1]　Daisuke Inoue[1]　Koji Nakao[1]

Abstract: Targeted attacks which aimed at a specific orgnization or company become an object of public concern. Targeted attacks have some attacking phases, for instance reconnaissance, installation exploitation and so on. According to some analyzing reports, attackers use various tools. Most of analyzing reports have results which include attacking tools and malwares individually. Therefore, relevances among the individual results are complemented of scenarios which analysts suppose, because analysts can not obtain attaking environments and harmful environments substantially. In this paper, we implement an environment for reproducing whole scenarios of targeted attacks in order to observing attackers' activities precisely. The environment has some attaking tools and a simulated C&C server as an attacker's zone. Also, we implement a victim's zone like a company's computing environment which is targeted from attackers. In addition, the environment has supporting zone which is used for reproducing attacking scenarios easily. At last, we produce a scenario of a targeted attack in this environment and discuss this environment with some logs such as Windows event logs, some server logs and network traffic data on the victim's zone.

1. はじめに

企業や政府のような特定の組織に狙いを定めて組織内の計算機環境の破壊や機密情報の収奪を目的としたサイバー攻撃，標的型攻撃が社会的な問題となっている．標的型攻撃の特徴として，目的を達成するまでに長期間にわたり段階的に攻撃を重ねることが挙げられる．この攻撃で用いられるマルウェアや RAT (Remote Administration Tool /

[1] 独立行政法人 情報通信研究機構 サイバー攻撃対策総合研究センター
Cybersecurity Research Center, National Institute of Information and Communications Technology, Koganei, Tokyo, 184–8795, JAPAN
[2] 株式会社セキュアブレイン 先端技術研究所
Advanced Research Laboratory, SecureBrain Corporation
[a)] tsuda@nict.go.jp

Remote Access Trojan) は標的組織用にカスタマイズされていたり，それ以外にも攻撃者は Windows OS に標準搭載されたコマンドやネットワーク管理者が利用する Windows Sysinternals[1] のようなツール群などを駆使するため，従来からのシグネチャマッチングやアノマリ検知のみでは攻撃者の振る舞いを見逃してしまう可能性がある．

現在，これらの攻撃ツールを中心とした標的型攻撃に関する解析レポートがさまざまなマルウェア解析ベンダから公開されている [2], [3], [4]．これらの解析レポートでは，攻撃ツールやマルウェアを静的解析したり，動的解析から得られたトラフィック情報の分析結果が個々にまとめられている．しかし一方で，標的型攻撃の一連の流れは，解析結果から得られた個々の事象を基に解析者が想定したシナリオで補完されている．これは解析者が攻撃を解析するときに，1) 攻撃者の環境の一部が停止しているため動的解析を十分にできない，2) 被害環境に残された攻撃の痕跡を収集することが難しい，といったことが原因となっている．さらに，標的型攻撃が発生する時期や攻撃個所，攻撃者の振る舞いは不定であるため，攻撃の様子をリアルタイムに観測して攻撃活動を分析することも難しい．

そこで本研究では，より正確に標的型攻撃における攻撃者の活動を把握するために，一連の標的型攻撃のシナリオを再現できる環境を構築する．シナリオ再現環境として，標的型攻撃の被害に遭う組織を模した環境と攻撃を実行する攻撃者の環境を共に構築する．被害環境としては企業組織の計算機環境を想定し，従業員の作業環境や組織内部で利用されるサーバ，組織外部への情報提供用のサーバを用意する．攻撃環境には，実際の攻撃後には既に停止していると思われる C&C サーバを模擬したものを実装する．その他に，被害環境や攻撃環境に用いられる機器やソフトウェアを柔軟に変更できる仕組みを構築し，多様な攻撃シナリオに対応できるようにする．

本環境を用いることで標的型攻撃の始まりから終わりまでの一連のシナリオを解析者の手元で再現できるようになる．これにより，一連の攻撃シナリオを追従し攻撃手法を解明することができる．また，被害環境の各種サーバや作業端末に残された攻撃の痕跡から被害の実態をより正確に把握でき，標的型攻撃対策の一助とすることができる．

本稿では，まず第 2 章で標的型攻撃対策に関する関連研究について述べる．次に第 3 章で本研究で提案する標的型攻撃シナリオ再現環境について述べる．そして，第 4 章では標的型攻撃の一つのシナリオを実施し，その結果より本提案環境について第 5 章で考察する．

2. 関連研究

2.1 標的型攻撃に関するレポート

本節では，各解析ベンダが公開した標的型攻撃に関するレポートを基に，いくつかの事例を紹介する．

Operation Aurora[2] は Internet Explorer の脆弱性を狙うゼロデイ攻撃によってコンピュータを乗っ取り，遠隔操作することで特定企業へ侵入した．これは Google 社を初めとした 30 以上の企業が攻撃対象とされ，メールのアカウント情報が収奪されるといった被害がもたらされた．

Night Dragon[3] は，エネルギー産業を狙った標的型攻撃である．標的企業の幹部に対してソーシャルエンジニアリングや RAT による遠隔操作，SQL インジェクションといった攻撃を組み合わせてコンピュータにアクセスし，各社の機密情報を狙った．この McAfee のレポートでは，侵入シナリオとして異なる想定シナリオを紹介している．

Mandiant が公開したレポート APT1[4] では，中国人民解放軍の部隊が関与し，数年に及び米国を中心とした企業や組織にスパイ活動をしていた事例について報告されている．ただし，中国人民解放軍が関与していると判断する根拠は状況証拠ばかりで，Mandiant の推測によるものが大きい．

これらのレポートでは，攻撃手法や攻撃の背景といった攻撃活動における個々の事象のつながりについては解析者が想定するシナリオで補完されている部分もあり，より正確な攻撃者の活動を把握することはこれらのレポートからでは難しい．

2.2 標的型攻撃対策に関する既存研究

標的型攻撃に特化した攻撃検知手法の研究も進められている．

山田らは組織内のネットワークトラフィックに着目し，標的型攻撃における諜報活動を早期検知する手法を提案している [5]．これは，ネットワークトラフィックの中でも Inbound 通信と SMB 通信開始，SMB 通信終了と Outbound 通信の連動に注目して不正な通信を検知する．

北澤らはマルウェアが侵入されたことを前提として，C&C サーバとマルウェア間の通信を検知して遮断する方法を提案している [6]．CAPTCHA のような認証機能によって，通信が人間の作業によって発生したものかマルウェアによるものかを判別し，通信を遮断するか否かを判断する．

これらの標的型攻撃対策の研究も前述した通り解析レポートを基に攻撃シナリオを想定して，対策すべき個所を絞って検知手法を提案している．一方で，標的型攻撃は攻撃者による被害環境への侵入から被害環境の機密情報を収奪するまでの流れは標的となる組織毎に異なり，攻撃活動は攻撃者が手動で実行することが多いことも広く知られており，今後攻撃者の活動も変化してくることが考えられる．このような標的型攻撃に対策を講じるためには，まず，標的型攻撃における攻撃者の活動を解析者・研究者が検証できる環境を構築し，攻撃活動の実態の把握と被害個所の特定を素早く行えることが重要であると考えられる．

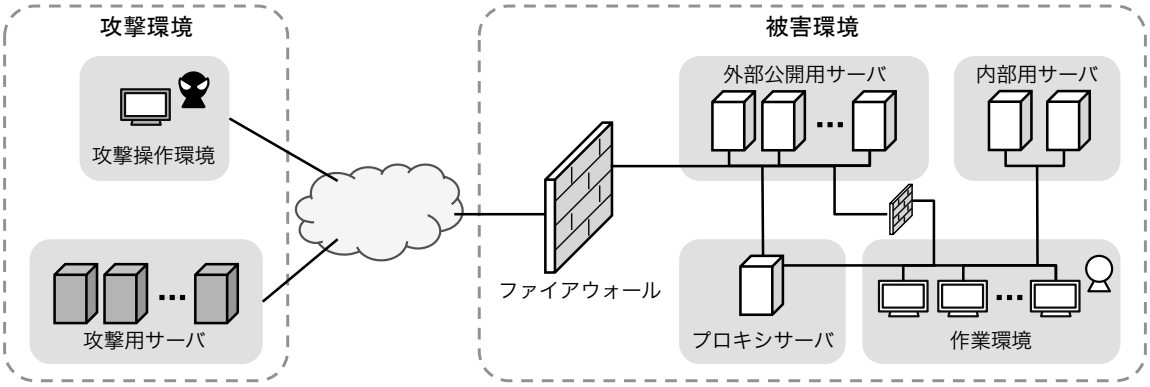

図 1 標的型攻撃のシナリオ再現時に登場する環境の一例

3. 標的型攻撃を対象としたシナリオ再現環境

3.1 概要

本研究では，標的型攻撃における攻撃者の振る舞いをより正確に把握するために，標的型攻撃の一連の流れを再現できる環境を構築する．図 1 に攻撃シナリオを再現する環境のモデルを示す．本環境は，大規模エミュレーション基盤 StarBED[7] を用いて構築する．攻撃シナリオ再現環境には標的組織を想定した**被害環境**と**攻撃環境**から構成される．この他に，解析者による攻撃シナリオ再現と攻撃の解析を支援する**解析支援環境**を持つ．

被害環境　攻撃の標的となる組織の計算機環境を想定する．その構成要素は，主に Windows OS が利用される**作業環境**，組織内部の人物が限定的に利用するファイルサーバや認証サーバなどの**内部用サーバ**，外部との通信を中継する**プロキシサーバ**や組織外部に情報を提供する WWW サーバのような**外部公開用サーバ**が挙げられる．

攻撃環境　標的となる組織に対して攻撃を仕掛けるために必要なものをまとめている．攻撃者が攻撃操作を実際に行う**攻撃操作環境**，組織内部に送り込んだマルウェアと通信しコマンドを実行する C&C サーバや追加でマルウェアをダウンロードさせるときに利用する WWW サーバを配置した**攻撃用サーバ**がある．

解析支援環境　被害環境および攻撃環境を柔軟に構築することを支援する環境で，攻撃シナリオを再現する上で必要なツール群が集められている．また，攻撃シナリオの再現により被害環境に残された攻撃の痕跡を収集する役割も持つ．

上記 3 種類の環境は StarBED 上のノードに KVM (Kernel-based Virtual Machine)[8] を用いた仮想環境として構築する．これにより被害環境・攻撃環境を柔軟に構築でき，攻撃シナリオの再現を反復して実行できる．

本研究では，シナリオ再現環境のひとつのモデルとなる被害環境と攻撃環境を構築し，攻撃シナリオの一例を実施する．以降の節では，その被害環境と攻撃環境，そして解析環境の詳細について述べる．

3.2 想定する被害環境

標準的な被害環境として，企業などの組織におけるひとつの部署を想定する．従業員が利用する作業環境端末には Windows XP SP3 および Windows 7 といった Windows OS がインストールされた計算機を用意する．これらは，それぞれ Active Directory を用いた認証サーバにドメイン参加し，ユーザ認証は Active Directory で集中して行う．また，特定の権限を持った従業員のみがアクセス可能なファイルサーバも同一のドメインに参加している．さらに，Active Directory ではドメイン参加する作業環境端末による各種イベントログも OS の基本設定で管理される．

作業環境端末から組織外への通信は柔軟に構成する．たとえば，ファイアウォール単体で組織外部への接続制限するような構成にしたり，プロキシサーバとファイアウォールを組み合わせて組織内・組織外への通信を制限する．

これらの構成要素は攻撃シナリオによって異なることが想定される．そのため，被害環境を柔軟に組み替えることも考慮しなければならない．この点については，Windows OS がインストールされた作業環境端末の台数や組織内に設置されたサーバ等は仮想マシン上で構築されるため，柔軟に組み換えられる．また，各仮想マシン間の通信は仮想ネットワークインタフェースを通るため，計算機を別のサブネットに参加させるといったことも容易に変更できる．

3.3 攻撃環境の再現

3.3.1 攻撃操作環境と攻撃用サーバ

攻撃操作環境には，Poison Ivy や DarkComet のような RAT や次節で述べる模擬 C&C サーバを操作するためのインタフェースが備えられている．攻撃者はこれらのインタフェースを通して被害環境へ侵攻するところから機密情報

表 1 模擬 C&C サーバに実装されたコマンド

コマンド	内容
shell	cmd.exe を起動
whoami	端末利用者の名前を取得
list	感染端末情報を取得
putf	感染端末へファイルを送信
getf	感染端末からファイルを受信
start	プログラムを開始
quit	C&C サーバとの通信を終了

を収奪し，攻撃の痕跡を消去する一連の流れを操作する．

攻撃用サーバには，標的型攻撃の一連のシナリオに必要となるものが揃えられている．たとえば，被害環境へ侵攻するための窓口を作るドライブ・バイ・ダウンロード攻撃（以下，DBD 攻撃）を実行するための Exploit Kit を設置した WWW サーバや，被害環境で機密情報の探索や攻撃活動するためのツール群を置いたファイルサーバ，被害環境に設置したマルウェアに命令を送る C&C サーバを模擬したものを設置している．

この他にも，被害環境に対して DBD 攻撃サイトの URL や文書型のマルウェアを添付したメールを送って攻撃を開始することもでき，多様な攻撃シナリオに対応できる．

3.3.2 模擬 C&C サーバ

攻撃者が遠隔から被害環境の計算機を操作する際には，被害環境にマルウェアを仕込み，C&C サーバから指令を送る方法がとられる．多くの標的型攻撃の場合，攻撃の被害に遭ったことを発見したときにはすでに C&C サーバは停止しており，解析者は正確に攻撃者の活動を把握することが難しかった．そこで本研究では，C&C サーバを再現することで攻撃活動をより正確に把握できるようにする．

模擬 C&C サーバには実検体から得られたコマンドが再現されている．具体的なコマンドは，実検体の静的解析の結果や実検体と C&C サーバとの通信内容，あるいは公開されている解析レポートから再現されている．今回は，Mandiant のレポート APT1[4] に記載されている検体 WEBC2-GREENCAT を静的解析して得られたコマンドを参考に模擬 C&C サーバを構築した．表 1 に模擬 C&C サーバに実装されているコマンドを示す．

これらのコマンドを利用することで，模擬 C&C サーバを通じて被害環境の計算機を遠隔操作し，機密情報を収奪するといった攻撃活動を実現できる．

3.4 柔軟な環境構築の実現

標的型攻撃における攻撃者の活動や被害環境の構成要素は多様であり，攻撃の解析を行うためには柔軟に被害環境および攻撃環境を構築することが要求される．

そのために，解析支援環境では攻撃シナリオに必要とされるツール群を管理する（図 2）．解析者は再現する攻撃シナリオに合わせて解析支援環境から被害環境・攻撃環境に対して必要なツールをインストールする．

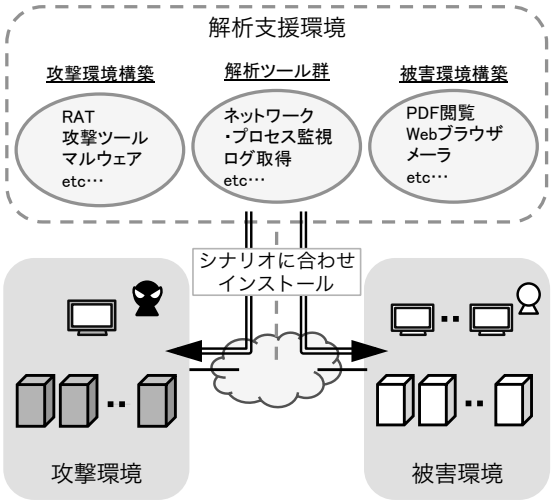

図 2 柔軟なシナリオ再現環境構築のための解析支援環境

解析支援環境は攻撃シナリオを実施する事前準備の段階では被害環境と攻撃環境に共に接続できるようにネットワークが構成されている．そして，攻撃シナリオを実施するときには解析支援環境を被害環境および攻撃環境から接続できないようにネットワークを隠蔽し，攻撃シナリオには影響を及ぼさないように運用する．

4. 標的型攻撃シナリオの実施

4.1 攻撃シナリオの概要

本研究では，構築した環境を用いて標的型攻撃のシナリオのひとつを再現し，被害環境のどの箇所にどのような攻撃の痕跡が残されるのかを調査する．

今回の攻撃シナリオ再現で用いた環境の構成を表 2 に示す．この環境は小規模な組織を想定して構成されている．作業端末やファイルサーバは Active Directory で認証される．また，作業端末から組織外部へ通信を行う場合はファイアウォールを経由する．

本研究で再現した攻撃シナリオは Mandiant APT1[4] を参考にして作成されたものである．なお，本研究ではシナリオの各フェーズを手作業で実行する．

(1) 攻撃者が DBD 攻撃サイトの URL が記載されたメールを送信する．その後，被害者が作業端末のうち 1 台で URL をクリックしマルウェア（WEBC2-GREENCAT）に感染する．

表 2 今回の攻撃シナリオ再現環境の構成

	用途		台数
被害環境	作業端末	Windows XP SP3	3
	ファイルサーバ	Windows Server 2012	1
	Active Directory	Windows Server 2012	1
	メールサーバ	Postfix, Dovecot	1
	ファイアウォール	iptables	1
攻撃環境	模擬 C&C サーバ	DBD 攻撃サイト	1

表 3 攻撃シナリオの各フェーズと被害環境に残された痕跡の対応

フェーズ	AD	FW	作業 (1)	作業 (2)	作業 (3)	再現内容
（諜報）	-	-	-	-	-	-
侵攻						メールの送信
潜伏		○	外部通信/プロセス			マルウェアのダウンロード・感染
橋頭堡確保		○	外部通信/プロセス			攻撃ツール群のインストール
索敵			内部通信/プロセス	通信	通信	組織内ネットワークを調査
（浸透）	-	-	-	-	-	-
占領	○		内部通信/プロセス			認証の突破
収奪		○	内部・外部通信/プロセス			機密情報を入手，C&C サーバに送信
撤収			プロセス			攻撃の痕跡の消去

(2) C&C サーバとマルウェアが通信を開始し，攻撃者は攻撃環境から被害環境の作業端末を遠隔で制御する．制御の内容は以下の通りである．
  (a) 攻撃ツール群を送り込む．
  (b) 被害者の他の作業端末およびファイルサーバを探索し，機密文書を感染した作業端末上に収集する．
  (c) 収集した機密文書を C&C サーバへ送信する．
  (d) 攻撃の痕跡を消去する．
(3) C&C サーバとマルウェアが通信を終了する．

今回の攻撃シナリオ再現において攻撃の痕跡を得るために，作業端末にはプロセスの監視に Windows Sysinternals の Process Monitor，ネットワークトラフィックの監視に Wireshark[9] をそれぞれインストールする．Active Directory では作業端末におけるユーザ認証がイベントログとして保存されている．また，作業端末が HTTP 通信する場合はファイアウォールを経由するため，そのログが保存される．

4.2 被害環境に残された攻撃の痕跡

表 3 に今回の標的型攻撃の再現において被害環境に残された攻撃の痕跡をまとめたものを示す．この表では，文献 [10] に記載されている標的型攻撃における 9 段階の攻撃フェーズに従い，各攻撃フェーズ・各計算機において残された痕跡をまとめている．Process Monitor で痕跡を発見したものには「プロセス」，Wireshark で発見したものには「通信」と表記し，組織内部での通信には「内部」，組織外との通信には「外部」と付記している．また，Active Directory やファイアウォールにログが残されていた場合には「○」を表記している．なお，再現した攻撃シナリオには諜報フェーズと浸透フェーズは含まれていないため，今回の調査からは除外する．

侵攻フェーズでは DBD 攻撃サイトの URL が記載されたメールが送信されるが，今回の環境では何も痕跡が得られなかった．

標的型攻撃の入口にあたる潜伏フェーズでは，Web ブラウザを開いて DBD 攻撃サイトからマルウェアがダウンロードされるときや，それに追加で C&C サーバからファイルをダウンロードするときにはファイアウォール経由で通信するためにその痕跡が残されていた．

組織内ネットワークでの攻撃活動が主となる橋頭堡確保，索敵，占領のフェーズでは組織内のネットワークを調査する通信を各作業端末で観測できた．たとえば，マルウェアに感染した作業端末から他の作業端末への通信や，認証のために Active Directory への通信がある．また感染した作業端末上でマルウェアによるプロセスの生成が観測できた．

そして最後に，標的型攻撃の出口にあたる収奪，撤収のフェーズでは機密情報のファイルを入手する SMB 通信や組織外部に機密情報を送信する際には HTTP 通信が作業端末でも発生しており，外部との通信の痕跡がファイアウォールで確認できた．

5. 考察

5.1 攻撃シナリオ再現から得られた知見

模擬 C&C サーバを実装することで残される痕跡の個所が各攻撃フェーズと対応して明らかとなった．たとえば，Active Directory でユーザ認証の痕跡が見られたことや組織外部にある攻撃環境のサーバと作業端末間で HTTP 通信を用いたときにはファイアウォールに痕跡が残されることを確認できた．今回の環境ではファイアウォールで通信を制限していたが，プロキシサーバを利用した場合には同様に痕跡が残されると考えられる．これらの攻撃の痕跡は今回の攻撃シナリオの元となった Mandiant APT1 レポートでは示されておらず，本環境での攻撃シナリオを再現したことにより確認できた事象である．

Mandiant APT1 レポートでは攻撃シナリオの各攻撃フェーズで攻撃者が用いたと思われる技術要素がいくつか紹介されている．実際に本環境でそれらの技術要素を組み合わせて攻撃シナリオを構成し，一連の流れで再現することで Active Directory やファイアウォールといった被害環境内の計算機に痕跡が残ることを改めて確認することができた．このように，攻撃シナリオを再現することで解析レポートには掲載されていない被害環境に残された攻撃の痕跡を洗い出すことができ，解析者が攻撃への対策を考察するときの一助となると考えられる．

また，本環境では被害環境の構成を柔軟に変更できるため，さまざまな規模の組織を想定して実験できる．たとえば，新たな標的型攻撃の解析レポートが公開されたときに，被害環境の規模や構成を変化させながら攻撃の痕跡を洗い出し，その傾向を即座に分析できる．

5.2 攻撃シナリオ再現から見えた提案環境の課題

本環境でひとつの攻撃シナリオを再現したことにより，本環境における課題も見えてきた．

本環境は柔軟に環境を構築し攻撃シナリオを再現することを目指しているが，その構築や攻撃シナリオの再現は現状では完全に自動化できていない．たとえば，環境構築時には，解析支援環境を用いて被害環境や攻撃環境に必要なツールをインストールするときには，それらのツールを解析者が選択しなければならない．攻撃シナリオ再現時には，解析者自身が攻撃環境で C&C サーバからコマンドを送信する，被害環境でメールを開封し URL をクリックするといった操作が必要となる．攻撃シナリオの再現を円滑に反復して実行できるようにするためには，攻撃環境・被害環境における解析者の操作もある程度自動化する必要があると考えられる．

また，現状の環境では攻撃シナリオに多様性を持たせられない．これは実際の標的型攻撃で利用された可能性があるマルウェア実検体を用いているためで，攻撃シナリオがその検体に依存するためである．たとえば，今回用いた検体では SMTP，HTTP，HTTPS の 3 種類のプロトコルでのみ通信するため，その他の通信プロトコルを利用した攻撃シナリオは現状の本環境では再現できない．この点については，多彩なプロトコルで模擬 C&C サーバと通信可能な「模擬マルウェア」を実装できれば，より多様な攻撃シナリオを構成することができると考えられるため今後の研究課題とする．これにより被害環境と攻撃環境に多様性を持たせることができ，実際に起こりうる攻撃活動の分析やそのときに残される攻撃の痕跡を調査できる．

被害環境に残された痕跡を分析するという観点では，本環境で攻撃シナリオを再現すると複数の計算機に攻撃の痕跡が大量に残るため，そこから解析者が攻撃の本質を見抜くために多大な労力を要する．著者らはこの課題を解決するために，複数の計算機を横断してプロセスの開始やネットワークへの接続といったあらゆる痕跡を一覧するシステムの開発を進めている [11]．今後は本環境と統合することで，攻撃シナリオの再現から攻撃の解析作業までを一貫して支援できるようにする方針である．

6. おわりに

本研究では，標的型攻撃における攻撃者の活動をより正確に把握するために，攻撃シナリオを再現する環境を構築した．シナリオ再現環境は，大きく分けて攻撃の被害に遭う組織を想定した被害環境と攻撃を仕掛けるために必要な物が集められた攻撃環境で構成され，標的型攻撃のシナリオに合わせて柔軟に構成を変更できる仕組みを持つ．

さらに，攻撃環境には，実際の標的型攻撃の被害発覚後には既に停止している場合が多い C&C サーバを模擬したものを実装した．これにより，公開されている解析レポートに記載されたシナリオを本環境で検証することができ，被害環境に残された攻撃の痕跡を分析することで標的型攻撃の対策を考察することが可能となる．

本研究では実際に提案した環境を用いて，Mandiant APT1 レポートを参考に攻撃シナリオを再現した．Mandiant APT1 レポートでは標的型攻撃で用いられた技術要素が紹介されているが，その技術要素と今回実装した模擬 C&C サーバを攻撃環境に置くことで，攻撃シナリオの一連の流れで被害環境に残される痕跡とその個所を改めて確認することができた．

本環境は現状では解析者がコマンドを実行する，URL をクリックするといった手動の作業が環境構築時や攻撃シナリオ再現時に発生する．攻撃シナリオの再現を反復するためには，このような作業を可能な限り自動化していく必要がある．さらに，多様なシナリオを再現するために，模擬 C&C サーバには SMTP，HTTP，HTTPS のみの限定的な実装ではなく，他の通信プロトコルも対象として研究開発を進めていく．また，本環境で得られた攻撃の痕跡を精査する環境も整備することで，攻撃シナリオの再現から攻撃の解析作業までを通して実施できる環境構築を目指す．

参考文献

[1] Windows Sysinternals. http://technet.microsoft.com/sysinternals/.
[2] McAfee. Protecting Your Critical Assets: Lessons Learned from “Operation Aurora”. Technical report, 2010.
[3] McAfee. Global Energy Cyberattacks: “Night Dragon”. Technical report, 2011.
[4] Mandiant. Mandiant APT1: Exposing One of China’s Cyber Espionage Units. Technical report, 2013.
[5] 山田正弘, 森永正信, 海野由紀, 鳥居悟, 武仲正彦. 組織内ネットワークにおける標的型攻撃の諜報活動検知方式. 2014 年暗号と情報セキュリティシンポジウム（SCIS2014）, 2014.
[6] 北澤繁樹, 河内清人, 桜井鐘治. 標的型攻撃におけるマルウェア通信の検知と対策. 2012 年暗号と情報セキュリティシンポジウム（SCIS2012）, 2012.
[7] StarBED. http://starbed.nict.go.jp/.
[8] KVM. http://www.linux-kvm.org/.
[9] Wireshark. http://www.wireshark.org/.
[10] 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　新型サイバー攻撃の検知と対応. 2012.
[11] 遠峰隆史, 津田侑, 神薗雅紀, 杉浦一徳, 井上大介, 中尾康二. 複数ホストを横断可能なタイムライン型イベントログ閲覧システム. Vol. 113, No. 502, ICSS2013-79, 2014.