標的型攻撃再現のための攻撃シナリオ定義インタフェースの実装

津田 侑† 神薗 雅紀†,‡ 遠峰 隆史† 安田 真悟† 三浦 良介†
宮地 利幸† 衛藤 将史† 井上 大介† 中尾 康二†

†独立行政法人 情報通信研究機構
184-8795 東京都小金井市貫井北町 4-2-1
{tsuda, masaki_kamizono, tomine, s-yasuda, myu2}@nict.go.jp
{miyachi, eto, dai, ko-nakao}@nict.go.jp

‡株式会社セキュアブレイン
102-0083 東京都千代田区麹町 2-6-7 麹町 RK ビル 4F
masaki_kamizono@securebrain.co.jp

あらまし 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．著者らはこれまで攻撃者の活動に伴って被害環境に残される痕跡を正確に把握するために，攻撃環境と被害環境を柔軟に構築できる標的型攻撃シナリオ再現環境を提案してきた．一方で，標的型攻撃における攻撃者の活動は多様なため，分析を繰り返し行うためには攻撃再現の効率化が求められる．そこで本稿ではシナリオ再現環境において，円滑に攻撃再現を進めるための攻撃シナリオ定義を支援するインタフェースを実装する．これにより 1）攻撃環境中の C&C サーバと被害環境内のマルウェアとの間のやり取り，2）被害環境内での攻撃ツールの実行手順の組み立てを効率的に行えるようになる．最後に標的型攻撃のケーススタディを実施し，考察を述べる．

Implementation of an Interface to Define Attacking Scenarios for Reproducing Targeted Attacks

Yu Tsuda† Masaki Kamizono†,‡ Takashi Tomine † Shingo Yasuda†
Ryosuke Miura† Toshiyuki Miyachi† Masashi Eto† Daisuke Inoue†
Koji Nakao†

†National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, JAPAN
‡SecureBrain Corporation.
2-6-7, Kojimachi, Chiyoda-ku, Tokyo 102-0083, JAPAN

Abstract Targeted attacks, a specific type of cyber-attacks targeted to a specific organization, are recognized as serious social concerns. It has been reported that the attackers are often activating by using various tools effectively in the several attacking phases. In the previous work, we have implemented an environment for reproducing targeted-attacks scenarios, which consists of victim zone and attack zone in order to precisely observe attackers' behaviors. In this paper, we implement an interface which support defining attacking scenarios with aim to reproduce targeted attacks effectively. To define an attacking scenario, at first, our interface supports defining communications between a C&C server in attack zone and a bot in victim zone. Secondly, it supports definition of attackers' behaviors in victim zone. In the last part of this paper, we describe case studies of targeted attacks and we discuss them.

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．標的型攻撃の目的は，組織内の機密情報の収奪や計算機環境の破壊などが挙げられる．これらのような目的を達成するまでに攻撃者は長期間にわたり段階的に攻撃を重ねることが知られている [1]．標的型攻撃で攻撃者が用いるツールには，既知または未知の脆弱性を狙うマルウェアや遠隔操作を実現する RAT (Remote Administration Tool / Remote Access Trojan) などがあるが，これらは標的とする組織用に特化したカスタマイズが施されていることもある．他にも攻撃者は 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[2] 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．

標的型攻撃対策の情報源として，標的型攻撃に用いられた攻撃ツールを中心とした解析レポートがさまざまなセキュリティベンダから公開されている [3, 4, 5, 6]．一般的に解析レポートでは攻撃ツールに関する解析は詳細に記述されている一方で，標的型攻撃が段階的に進む様子や各攻撃段階間の関連は解析者の想定で補完されている．これらは，標的型攻撃の事後では，攻撃者の環境が既に停止されていたり，被害者の環境下で攻撃の痕跡を収集することが困難であることが原因として考えられる．

そこで著者らはこれまで，より正確に標的型攻撃における攻撃者の活動や被害組織に残された攻撃の痕跡を把握することを目的として，標的型攻撃の一連のシナリオを再現できる解析環境（以下，**シナリオ再現環境**と呼ぶ）を構築してきた [7]．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．攻撃環境には，模擬 C&C サーバを設置することで，シナリオ再現環境内のみで攻撃シナリオの実行を完結させることができる．

これまでのシナリオ再現環境では，攻撃環境および被害環境を柔軟に構成変更できる仕組みは持っていたが，その上で攻撃シナリオを再現するには手作業で行う部分が多かった．たとえば，攻撃環境の C&C サーバから被害環境のマルウェアへコマンドを送信したり，被害環境内でネットワークの探索や他ホストへ侵攻する場合には解析者自身が操作する必要があった．これでは，解析者が様々な攻撃パターンを再現しようとしても，多彩な手法で攻撃が進められる標的型攻撃を分析するためには多大なコストを要する．そこで本稿では，これらの課題を解決するために，攻撃シナリオの組み立てを支援する仕組みを提案する．これにより，より円滑に多様な攻撃シナリオを反復して再現することが可能となる．

本稿の構成は以下の通りである．第 2 章ではまず，標的型攻撃対策に関する既存研究について述べる．そして次に本稿の先行研究となる標的型攻撃シナリオ再現環境について述べる．第 3 章では，本稿で提案する攻撃シナリオ再現支援の仕組みについて述べる．そして，第 4 章では標的型攻撃のシナリオをケーススタディとして実施し，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　攻撃活動を「知る」ための取り組み

これまで，標的型攻撃対策のために攻撃者の活動を把握しようとする取り組みが数多くなされてきた．

まず，攻撃者の活動を模擬する試みがある．攻撃者が用いるマルウェアやそれに命令を送る C&C サーバの基本的な機能を模擬的に実装した ShinoBOT/ShinoC2[8] や HAGRAT[9] は，セキュリティアプライアンス製品や各種検知エンジンの検証に用いられる．

また，Guri らは OpenAPT という枠組みを提案している [10]．この枠組みでは，既知の攻撃方法（コードの難読化やマルウェア感染手法，アンチフォレンジック手法など）をモジュール化して提供する．各モジュールを組み合わせる

ことで模擬的な攻撃を実現することができ，新たな標的型攻撃対策手法の実験・評価に用いることができる．

これらの取り組みは，攻撃者の活動を模擬することで標的型攻撃に対する施策を検証することを目的としている．一方で，著者らは攻撃者の活動を把握することに加え，攻撃者が活動する中で被害組織に残されていく痕跡を精査・分析することを目的として標的型攻撃の一連のシナリオを再現できる環境の構築を進めている．

2.2 標的型攻撃シナリオ再現環境

攻撃者の活動を把握することに加え，被害組織に残された攻撃活動の痕跡を詳細に分析することを目的として，著者らは標的型攻撃のシナリオ再現環境 [7] を構築してきた．シナリオ再現環境は大規模エミュレーション基盤 StarBED[11] 上に仮想マシンおよび仮想ネットワークとして構築されている．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．

被害環境は標的となる組織の計算機環境を模している．組織の構成員が利用する Windows OS が導入された計算機の他に，ファイルサーバや認証サーバ，プロキシサーバなど組織内で利用されるサーバ群を持つ．攻撃環境は，標的となる組織に攻撃するために必要なものの集合体である．ドライブ・バイ・ダウンロード攻撃サイトや攻撃ツール群が設置された WWW サーバの他に，組織内部に送り込んだマルウェアに命令を送信する C&C サーバも持つ．

解析支援環境は，被害環境および攻撃環境の柔軟な構成変更を支援する．各環境にインストールするソフトウェアや攻撃シナリオ再現後に被害環境からログを収集する役目を持つ．この解析支援環境は攻撃シナリオ再現中には被害環境および攻撃環境からは分離されるため，攻撃シナリオ再現には影響しない．

これまでのシナリオ再現環境では，被害環境および攻撃環境を柔軟に構築することに焦点を当ててきた．それゆえに，攻撃シナリオを再現するときには解析者自身が手作業で操作する部分も多く存在した．本稿では，再現する攻撃シナリオを定義するインタフェースを開発し，再現を効率的に実施可能とすることを目的とする．本稿が目指すシナリオ再現環境の概要を図 1 に示す．このインタフェースにより，解析者は多様な攻撃シナリオを簡便に組み立てることができ，被害環境の構成を変更させながら反復して攻撃シナリオを再現することで効果的なケーススタディを実施できる．

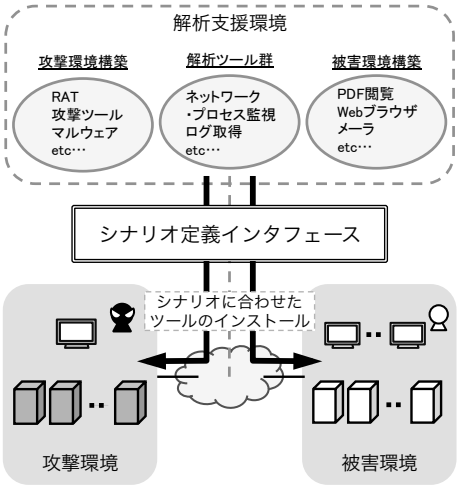

図 1: 標的型攻撃シナリオ再現環境

3 シナリオ定義インタフェースによる攻撃再現支援

3.1 シナリオ再現までの流れ

シナリオ再現環境を用いて攻撃シナリオを再現するまでの流れは以下の通りである．

1. 攻撃環境・被害環境の設定
2. 被害環境内での活動の定義
   - 各攻撃フェーズで用いるツールの選択
   - 選択したツールを用いたバッチ処理
3. C&C サーバとの通信の定義
   - C&C サーバからのコマンドの選択
   - 通信開始から終了までの処理手順
4. 攻撃シナリオ再現を実施

表 1: 被害環境内での各攻撃フェーズで利用されるツール例（下線は OS 標準搭載）

フェーズ	説明	ツール例
潜伏	標的内部の PC に入り込む	DBD 攻撃サイト，文書型マルウェアなど
橋頭堡確保	標的内部の PC を支配	C&C サーバと通信するマルウェア
索敵	ネットワーク情報の探索	ping, net など
浸透	ネットワーク内に踏み台を増殖	各種 RAT（PoisonIvy など）
占領	目的となるサーバの支配	pwdump, gsecdump, wce など
収奪	目的情報の入手と搬出	winrar, zxhttpserver など
撤収	攻撃の痕跡の消去	del, sdelete, elsave など

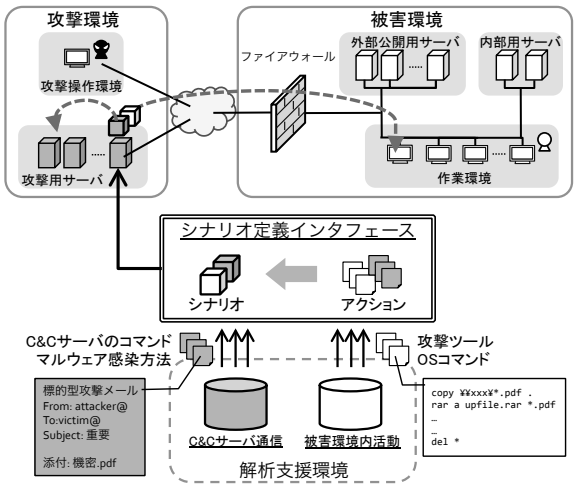

図 2: シナリオ定義インタフェースの概要

まず，実行したい攻撃シナリオに合わせて攻撃環境・被害環境を設定する．次に，被害環境内での攻撃者の活動を定義し，被害環境内での活動をバッチ処理できるようにする．この内容を含めて，攻撃環境と被害環境の間で行われる通信を定義する．そして，これらを合わせて一連の攻撃シナリオとし，シナリオ再現環境内で動作させる．

この流れの中でも，「1. 攻撃環境・被害環境の設定」,「4. 攻撃シナリオ再現を実施」については著者らの先行研究である文献 [7] で提案してきた．本稿ではさらに攻撃シナリオの効率的な再現を目指して「2. 被害環境内での活動の定義」および「3. C&C サーバとの通信の定義」を実現するインタフェース（以下，**シナリオ定義インタフェース**と呼ぶ）を実装する．

ここで，シナリオ定義インタフェースを用いて攻撃シナリオを設計する上で，攻撃者による攻撃ツールの実行や C&C サーバからのコマンドの送信といった一つ一つの細分化された行動を**アクション**と呼ぶ．そして，アクションを複数合わせて組み立てられた攻撃の一連の流れを**シナリオ**と呼ぶ．一度記述したアクションおよびシナリオは再利用可能とし，既存のアクションや新規で作成したアクションを組み替えることよって全く新しいシナリオを作成することができる．図 2 はシナリオ定義インタフェースによってシナリオを作成し，それをシナリオ再現環境に投入する様子を示している．投入されたシナリオにより順次適切な場所にマルウェアや攻撃ツールが配置され攻撃が進行していく．

次節以降では，被害環境内での活動および C&C サーバとの通信それぞれについてのアクション・シナリオの定義方法を述べる．

3.2 被害環境内での活動の定義

標的型攻撃の被害組織内での攻撃活動では，各攻撃フェーズごとに用いられる攻撃ツールがあり，さらには OS 標準搭載のコマンドが攻撃活動に利用されることが知られている．表 1 に各攻撃フェーズごとのツールの一例を挙げる．なお，これらの攻撃フェーズの分類は文献 [1] に倣っている．

被害環境内での活動の定義では，まず，これらのツールやコマンドの利用方法をアクションとして，コマンドラインのオプションを含めた単体のバッチファイルを記述する．そして，各

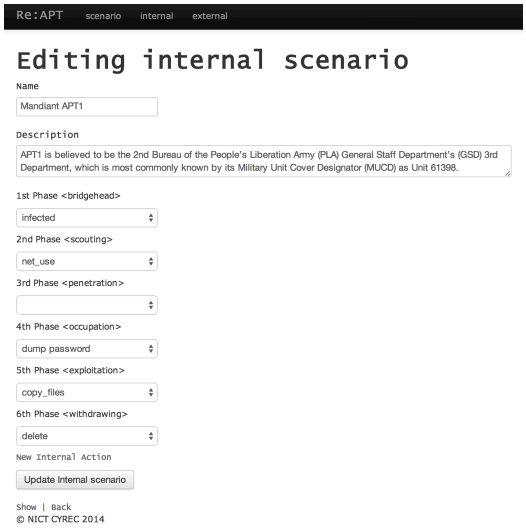

図 3: 被害環境内シナリオ定義インタフェース

攻撃フェーズごとにアクションを選択し，被害環境内でマルウェアに感染してから情報の収奪といった目的達成までの一連の攻撃シナリオを設計することで，それをシナリオ全体のバッチファイルとして出力する．このときバッチファイルおよびそのバッチファイル内で呼び出される攻撃ツールはアーカイブファイルとしてまとめられ，そのままシナリオ再現環境に投入できる．

これらの操作は図 3 のような Web インタフェース上で実施することができる．アクションの定義は，攻撃フェーズとその攻撃活動のバッチファイルを選択するのみで行える．バッチファイルはあらかじめ登録されたものを用いるか，もしくはその都度作成する．そして，こうして作成されたアクションを組み合わせることでシナリオを定義できる．この画面では攻撃フェーズ毎にアクションを選択でき，その組み合わせは自由に変更できる．

3.3 C&C サーバとの通信の定義

前節では，被害環境内でのアクション・シナリオの定義を述べた．本節では，C&C サーバと被害環境の間の通信の定義方法について述べる．この通信が定義されることにより，被害環境内のシナリオやそれに用いられる攻撃ツールを被害環境に投入したり，被害環境内から C&C サーバにファイルを収奪するといったことを実行できる．

表 2: C&C サーバ通信のアクションの種類

アクション	説明
response	要求への応答（コマンド送信）
upload	マルウェアへのファイル転送
download	C&C サーバへのファイル転送
sendmail	メールの送信

```
{
 "comment" : "メールの送信",
 "request" : [ {"text" : "*"} ],
 "sendmail": {
   "from"   : "attacker@example.net",
   "to"     : "victim@example.com",
   "subject": "this is a nice site!",
   "message": "http://malicious.example.net/xxx.exe",
   "attachment": "/home/attacker/malicious.pdf",
 }
}
```

図 4: sendmail アクションの一例

```
{
 "comment": "被害環境へ設置する攻撃ツールの設定",
 "request": [ {"text" : "GET"} ],
 "upload" : {"path" : "/home/attacker/tools.zip"}
}
```

図 5: upload アクションの一例

シナリオ再現環境内に実装された C&C サーバはマルウェアからの要求に応答して，表 2 に示す 4 種類のアクションを実行させることができる．response アクションはマルウェアからの要求に応答するもので，その応答にマルウェアへの命令を載せることでマルウェアを制御できる．upload, download アクションは送受信するファイルを設定するアクションで，sendmail アクションはメールの送信を実現する．これらのアクションが実行される条件は，マルウェアからの要求（文字列）に指定した正規表現で一致するかどうかで決まる．また，アクションの実行にはそれぞれのアクションごとに決められたパラメータを伴う．

ここではアクションの具体的な記述方法としてメールを送信する sendmail アクション（図

```
{
 "comment": "ファイル送受信のシナリオ",
 "port": 443,
 "action": [
 {
  "comment": "被害環境へ設置する攻撃ツールの設定",
  "request": [ {"text" : "GET"} ],
  "upload" : {"path" : "/home/attacker/tools.zip"}
 },
 {
  "comment": "tools.zip 展開のための unzip.exe",
  "request": [ {"text" : "GET"} ],
  "upload" : {"path" : "/home/attacker/unzip.exe"}
 },
 {
  "comment": "被害環境からファイル収奪",
  "request": [ {"text": "GET"},
               {"param1": "Content-Length"},
               {"param2": "FileSize"} ],
  "download": {"size": "param1",
               "FileSize": "param2",
               "path": "/home/attacker/files.rar"}
 } ]
}
```

図 6: C&C サーバの通信シナリオの一例

4）と被害環境内へ転送するファイルを設定する upload アクション（図 5）の一例を挙げる．C&C サーバは JSON 形式で記述された通信アクションを解釈し，マルウェアとの間の通信を規程できる．

sendmail アクションの例では，送信先アドレス（*victim@example.com*）に対して件名と本文を設定して送信している．また，ファイルを添付する場合は，そのファイルパスを指定する．

upload アクションの例では，*tools.zip* を被害環境へ設置する設定が記述されている．upload アクションのパラメータには，C&C サーバ上の攻撃ツール群のファイルパスを指定する．そして，被害環境内のマルウェアから GET 要求があった時にマルウェア側に攻撃ツール群が渡る．

次に，前述したアクションを適宜組み合わせてシナリオを構成する．これにより，C&C サーバからコマンドを送信して追加で攻撃ツールをダウンロードさせる場合や，目的となる情報をサーバにアップロードするといった被害組織内と C&C サーバの間のやり取りを実現することができる．

具体例として，図 6 に 443 ポート（HTTPS）を利用して送受信するファイルを設定するシナリオを挙げる．シナリオに記載されたアクションは，マルウェアからの要求がきたときに上から順番に実行される．図 6 では，まず最初にマルウェアから 443 ポートを用いた要求がきたときに，マルウェア側に設置するファイルとして C&C サーバ上の */home/attacker/tools.zip* を設定する．この *tools.zip* が前節で作成したアーカイブファイルにあたる．そして，別途マルウェア側にファイルをダウンロードするコマンドを発行することにより，マルウェア側にファイルを設置できる．そして同様に */home/attacker/unzip.exe* を設置する．ここから順次 C&C サーバ側からマルウェアにコマンドを送ることにより *tools.zip* が展開され，被害環境内での活動として定義したシナリオが進んでいく．最後に，被害環境内から収奪したファイルを C&C サーバに設置する場所を設定し，C&C サーバからマルウェアに対してファイルをアップロードするコマンドを発行することによりシナリオが完結する．

以上の C&C サーバとの通信定義も被害環境内のアクション・シナリオと同様のインタフェースがあり，あらかじめ定義したアクションを自由に組み替えることによって新たなシナリオを作成できる．

4 攻撃シナリオの再現

4.1 シナリオ内容

前章で述べたシナリオ定義インタフェースを用いて，標的型攻撃のシナリオを再現するケーススタディを実施する．シナリオは標的となる組織から機密情報を収奪することを想定する．被害環境内におけるシナリオの作成には Mandiant APT1[5] を参考に攻撃ツールを選定し，その攻撃ツールやコマンドを 2 パターンの異なる組み合わせで用意する．

表 3 にそれぞれのシナリオの各攻撃フェーズの内容と利用する攻撃ツール・コマンドを示す．また，ケーススタディのための被害環境として簡素なものを用意する．その構成を表 4 に示す．攻撃環境には文献 [7] で提案した模擬 C&C サーバを用いる．

攻撃シナリオは，潜伏フェーズにおいて攻撃環境から被害環境に向けてマルウェアを送り込むことから始まる．マルウェアに感染後，橋頭

表 3: 再現する攻撃シナリオの内容と利用ツール

フェーズ	内容	パターン（1）	パターン（2）
潜伏	被害環境内でマルウェアの実行	DBD 攻撃サイト [1]	文書型マルウェア
橋頭堡確保	C&C サーバとの通信を確立	WEBC2-GREENCAT	WEBC2-GREENCAT
索敵	ファイルサーバの探索	net コマンド	ping コマンド
浸透	（本稿では対象としない）	-	-
占領	感染端末のパスワードの奪取	wce	gsecdump
収奪	ファイルの収集，転送	winrar	7za
撤収	攻撃の痕跡を削除	del コマンド	sdelete

表 4: 被害環境の構成

用途	OS・サービス
作業端末	Windows XP SP3
ファイルサーバ	samba
メールサーバ	Postfix, Dovecot
ファイアウォール	iptables

堡確保フェーズで C&C サーバとマルウェア間の通信が確立され，被害環境に以降の攻撃フェーズで利用される攻撃ツールがダウンロードされる．索敵フェーズでは被害環境内にあるファイルサーバを探索する．その次に占領フェーズとして，マルウェアに感染した端末のパスワードを奪取する．そして，ファイルサーバから機密情報を収集，奪取したパスワードと合わせてアーカイブファイルを作成し，C&C サーバに転送する．最後にマルウェアや攻撃ツールを感染端末から削除する．

4.2 従来のシナリオ再現環境との比較

先行研究 [7] での攻撃シナリオの再現では，C&C サーバからマルウェアに対してメールを送る，何らかのコマンドを実行させるといったことをする場合，その都度 C&C サーバから操作を行う必要があった．また，被害環境内での攻撃活動も解析者自身が攻撃ツールをコマンドラインに入力して実行していた．

[1] ドライブ・バイ・ダウンロード攻撃サイト

本稿で提案したインタフェースを用いると，C&C サーバの通信や被害環境内での攻撃活動の一つ一つのアクションがモジュール化されるため，一度登録されたものであればインタフェース上で選択するのみで利用でき，シナリオに多様性を持たせることも簡便になる．

今回の攻撃シナリオ再現では Mandiant APT1 に記載されているものを参考にした 2 パターンのシナリオを用意したが，アクションを新たに定義することで他の解析レポートに記載されている攻撃シナリオも再現可能となり，しかも様々なアクションの組み合わせで容易に試行することができる．

5 考察

本提案インタフェースにより，事前にアクション・シナリオを定義してシナリオ再現環境で攻撃活動を自動的に実行できるようになる．これにより解析者が手作業で攻撃ツールやコマンドを実行することがなくなり，定義した通りに攻撃シナリオを開始から終了まで一貫して確実に再現できる．一方で，途中で攻撃が失敗したときに目的達成までの道筋から迂回して何らかの活動を行ったり，手戻りが発生したときの攻撃者の活動などは再現し難くなる．このような場合も考慮しつつ今後インタフェースを設計していく必要がある．

また，本稿で実現したインタフェースにより攻撃者の一連の活動をシナリオとして定義し，そのシナリオを自動実行できるようになったが，

被害者による能動的なアクションは実現できない．たとえば，攻撃者が被害環境に侵入するきっかけとなる被害者によるドライブ・バイ・ダウンロード攻撃サイトへのアクセスや，文書型マルウェアを開くといった動作は依然として解析者が模擬して手作業で行う必要がある．より効率的に攻撃シナリオを再現するという観点からは完全な自動化が望まれるが，この点についての議論は今後の課題とする．

6 おわりに

本稿では，これまで著者らが提案してきた標的型攻撃シナリオ再現環境の上で，攻撃シナリオの組み立てを支援する仕組みについて述べた．被害環境内の攻撃については，攻撃者の活動で用いられる攻撃ツール・OS 標準搭載のコマンドを自由に組み合わせて一連のシナリオを定義できるインタフェースを開発した．C&C サーバと被害環境間の通信についても，同様にインタフェース上で一連のシナリオを定義できる．それぞれの通信内容は JSON 形式で記述する．

また，本稿で提案したインタフェースを用いて，ケーススタディとして標的型攻撃の一連のシナリオ再現を試行した．攻撃シナリオは Mandiant APT1 のレポートに記載されたものを参考に構成し，利用する攻撃ツールやコマンドを変更した 2 パターンを作成した．提案したインタフェースにより，利用する攻撃ツールやコマンドの変更を容易にし，多様な攻撃シナリオを効率的に試行できるようになった．

今後は，提案インタフェースを用いて再現する攻撃シナリオを多様化させ，ケーススタディを実施する．それにより，標的型攻撃において重要となる対策箇所を見極め，その知見を活かして標的型攻撃対策の研究を推進していく．

参考文献

[1] 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.

[2] Microsoft. Windows Sysinternals. http://technet.microsoft.com/sysinternals/.

[3] McAfee. Protecting Your Critical Assets: Lessons Learned from “Operation Aurora”. Technical report, 2010.

[4] McAfee. Global Energy Cyberattacks: “Night Dragon”. Technical report, 2011.

[5] Mandiant. Mandiant APT1: Exposing One of China’s Cyber Espionage Units. Technical report, 2013.

[6] Olivier Bilodeau, Pierre-marc Bureau, Joan Calvet, Alexis Dorais-joncas, Marc-Étienne M Léveillé, and Benjamin Vanheuverzwijn. Operation Windigo - The vivisection of a large Linux server-side credential stealing malware campaign. Technical report, 2014.

[7] 津田侑, 神薗雅紀, 遠峰隆史, 安田真悟, 三浦良介, 宮地利幸, 衛藤将史, 井上大介, 中尾康二. 標的型攻撃のシナリオ再現環境の構築. 第 65 回コンピュータセキュリティ研究発表会, 2014.

[8] Shota Shinogi. ShinoBOT/ShinoC2. http://www.blackhat.com/us-13/arsenal.html#Shinogi.

[9] Markku-Juhani O.Saarinen. Developing a Grey Hat C2 and RAT for APT Security Training and Assessment. In *Proceedings of the GreHack 2013*, 2013.

[10] Mordehai Guri, Tom Sela, and Yuval Elovici. OpenAPT – Open-Source Advanced Persistent Threat for Academic Research (POSTER). In *Proceedings of the 34th IEEE Symposium on Security and Privacy*, 2013.

[11] StarBED. http://starbed.nict.go.jp/.