脅威トレースの攻防戦化

神武　克海[1,a)]　小出　洋[1,b)]

概要：情報化社会への変遷とともに，攻撃者による攻撃は標的型攻撃など悪質なものになりつつある．そのような攻撃に対しては，攻撃者の視点を得ることが有効な対策となる．攻撃者の視点は，実際の攻撃を模した環境上で攻防戦を行うことで効率的に獲得可能であるが，従来の攻防戦は，複雑で理解が進みにくく，高コストであると言う問題がある．そこで本稿では，脅威トレースと呼ばれるネットワークシミュレータの攻防戦化を行うことで，情報システムの設計者や管理者が攻撃者側の視点を得ることを支援する．攻防戦化により，低コストで抽象度が高く理解が進みやすい攻防戦が行える．我々は拡張後の脅威トレース上で十分攻防戦が行えることを確認した．

Applying Tracing Attacks on Advanced Persistent Threat in Networked Systems to Attack and Defense

Katsumi Kotake[1,a)]　Hiroshi Koide[1,b)]

Abstract: As the growth of the information society, the new type of cyber attacks (Advanced Persistent Threat, APT) are increasing. To counter it, to gain an attacker's perspective is effective. It is possible to gain it in Attack and Defense (battle). However, previous methods of Attack and Defense is complexity and costly. Therefore in the present study, we improve "the network simulator called Tracing Attacks on Advanced Persistent Threat in Networked Systems" to support gaining an attacker's perspective. We confirmed that it is possible to carry out the Attack and Defense.

1. はじめに

本研究の目的は，情報システムの設計者や管理者が，攻撃者の視点を得ることを支援することである．

1.1 背景

情報化社会への変遷とともに，悪意のある攻撃者によるサイバー攻撃が増加している．従来の攻撃は，不特定多数を対象とした攻撃やいたずら目的の攻撃が主であったが，近年の攻撃は非常に悪質で，特定の企業や組織・個人を狙い高度な攻撃が行われる傾向がある．その攻撃は執拗で，事前の調査が細かく行われ，綿密な計画を立てた上で行われることが多く，その性質から標的型攻撃や APT 攻撃（Advanced Persistent Threat）と呼ばれる [1][2].

[1] 九州工業大学
福岡県飯塚市川津 680-4 820–8502 , Japan
[a)] zip@klab.ai.kyutech.ac.jp
[b)] koide@ai.kyutech.ac.jp

そのような攻撃は，従来のような「入口対策」と呼ばれるファイアウォールやアンチウイルスソフト等では侵入を防ぐことが難しい．攻撃者はゼロデイ脆弱性やソーシャルエンジニアリングなど高度な技術を使用するため，情報システム内へ侵入されることを前提とした，「出口対策」と呼ばれる対策によって防御を行わなければならない．出口対策とは，攻撃者が侵入したとしても，情報流出を防ぐ対策であり，ネットワークの構成の再考や各サーバー設定の確認によって強固なシステムにする対策である．

出口対策を行う上で重要な要件として，攻撃者の視点を獲得することが挙げられる [3]．ネットワークの再構成を行う段階やサーバー設定の確認を行う段階で，攻撃者の視点を取り入れ，ネットワーク内のどの部分が攻撃対象となりやすいかや，どの部分が脆弱点でどのような対策を行えばよいか等は，攻撃者の視点を得ることで効率的にかつ効果的に行うことが可能である．

1.2 攻防戦

攻撃者の視点は，CTF(Capture The Flag) や攻防戦に参加し，実際に攻撃側や防御側となることで効率的に獲得可能である．そのため，世界各地で攻防戦大会や演習，研究が行われている．また，そのような攻防戦では，あるシナリオを想定し，そのシナリオに沿って攻防戦を行うことが多い．シナリオに沿った演習は自衛隊や他国の軍などでも使用されており，攻撃者の視点を得るために非常に重要な考え方である．

しかしながら，従来の攻防戦は複雑な攻撃手法や大量の知識が必要であり，攻撃者の視点を得るには不向きな場合がある．また，実際に実物の機器や仮想マシンを使用する場合が多く，次の様な問題がある．

- 開催コストが高い
- 複雑な攻防戦となるほど理解が進みにくい場合がある
- 行われた事象の追跡やログの確認が難しい

特に，攻防戦を競技の一種として捉える場合，難易度の高い技術や高度な知識を要求されることが多く，攻撃者の視点を得ることは難しい場合も多い．とくに，SECCON[4] 等で行われる攻防戦は問題や競技が高度になりやすく，理解が進みにくい場合がある．また，参加者はローカル環境に集められ，実際の機器やネットワークを構築して行われるため，高コストであることや，大量のログが分散して配置されるため，攻撃のトレースが行いにくいという問題がある．また，米 Boeing 社が開発している CRIAB(Cyber-Range-in-a-Box)[5] は，不正アクセスや改竄など，様々なセキュリティインシデントに対処する一連の流れ（シナリオ）を演習形式で体験することが可能であるが，実際の機器を用意する必要があり，非常に高コストである．また，防御面に重点が置かれており，攻撃者の視点を得ることが難しいと考えられる．

1.3 脅威トレースの攻防戦化

本研究では，脅威トレース上で攻防戦が行えるように改良を行う．脅威トレースとは，情報システム上でのマルウェアの挙動を網羅的に探索し，脆弱性を調査するネットワークシミュレーターである [6]．脅威トレースはソフトウェア上で情報システムを模擬しているため，攻防戦を行う上でコストを低く抑えることが可能である．また，情報システムモデルやツール等の抽象度が高く設定されているため，情報セキュリティの知識が少ない技術者でも理解が容易な攻防戦が行える．それに加え，脅威トレースに備わっているシミュレート機能を活用することで，抜け道のないシナリオを想定し攻防戦を行うことが可能である．

攻防戦化にあたり，実際の攻防戦に参加し得られた知見や攻防戦の運営となり得られた知見，また，各機関が発行している資料を元に，攻防戦で必要であると思われる機能を，脅威トレースに付け加える形で実装した．実装は，脅威トレース本体のメイン関数を攻防戦用のサーバープログラムへと変更することで，脅威トレースの本体のコードをそのまま流用可能な設計にした．サーバープログラムは主に脅威トレースのエンジンの利用と，クライアントからの入力の受け付けや出力，内部データの保持を行う．クライアントプログラムは，サーバーへの接続やプレイヤーからの入力をサーバーへと送信，出力の受信を行う．さらに，プログラミング言語 Scala[7] のアクターモデルを採用し，非同期で動作させることで実際のシェル端末のような操作で攻防戦を行えるように改良した．また，管理者側・攻撃側・防御側で別れてシェルを使用できる機能を追加し，それぞれのシェルで異なるコマンドを実行可能にした．

評価は，実際に発生した標的型攻撃に基づき攻防シナリオを作成し，そのシナリオに基づき最低限必要な機能を列挙し，攻防戦としてシミュレート可能であるかを確認することで評価した．その結果，概ね攻防戦で必要な機能を実装していたが，一部の機能に不足があるという検証結果となった．しかしながら，脅威トレースの機能を用いることや，脅威トレース改良後の攻防戦フレームワークの改良を行うことで，模擬可能であると考えられる．そのため，脅威トレース上で攻防戦が模擬可能であり，攻撃者の視点を得ることが可能であると考えられる．

2. 標的型攻撃

昨今の社会の情報化は目覚ましく，様々な企業や組織・個人がコンピュータを利用し，インターネット上で多様な活動を行っている．多くのデータが電子化され，個人情報をはじめとした隠匿すべき重要なデータもサイバー空間上で常に行き交っており，データの電子化は我々の生活に無くてはならない存在となっている．それに伴い，電子化された重要な情報の窃取を試みる等，いわゆる「サイバー攻撃」が増加しており，社会問題となっている．サイバー攻撃は情報システムの設計やプログラムの脆弱性を突き，データの破壊や窃取・改竄等を試みる攻撃であり，スパムメールやフィッシングメールを始め，ネットワーク盗聴やサービス拒否攻撃（DoS 攻撃/DDoS 攻撃）などが挙げられる．このような攻撃は近年増加傾向にあり [8]，大手企業や官公庁もサイバー攻撃により Web サイトの改竄や情報流出などの被害を受けている．

サイバー攻撃の中でも特に，特定の企業や個人を狙って行われる攻撃は「標的型攻撃」と呼ばれ，通常のサイバー攻撃と比較すると非常に高度で執拗な攻撃である．このような攻撃は従来と比較し，ゆっくりと時間をかけて行われる攻撃であるため，事前に様々な調査や試行が行われることが多い．また攻撃そのものも，対象に特化した特別なマルウェアやゼロデイの脆弱性が使用される等非常に洗練された攻撃手法であることが多々ある．そのため，標的型攻撃はアンチウイルスソフトやファイアウォールソフト等と

いった従来の方法（入口対策）では防御することが困難である．

2.1 攻撃手法

従来のサイバー攻撃は，クレジットカードや銀行会社のログインサイトを装い，クレジット番号や個人情報を抜き取る攻撃や，特定のサイトを改竄し，そのサイトを閲覧したユーザーに対しマルウェアの強制ダウンロードを試みる攻撃といった，不特定多数を対象とした攻撃が主であった．それと比較し，標的型攻撃は特定少数を対象として攻撃を実行するため，段階を踏み攻撃が行われるという特徴がある．

2.2 標的型攻撃の対策

標的型攻撃は入念な調査が事前に行われるため，従来の手法である入口対策だけでは情報流出を止めることはできない．そのため，攻撃から情報システムを防御するには，入口対策に加えて出口対策が必要となる．出口対策は内部対策とも呼ばれ，たとえ攻撃者を情報システム内部に侵入させてしまったとしても，情報を流出させないような設計にする対策である．攻撃者が必ずネットワーク内部に侵入してくることを前提にネットワーク構成・サーバーのセキュリティ設定などを設計することで，情報流出を抑えることが可能である．

標的型攻撃に有効な対策の例として，以下のような対策が挙げられる．

- ネットワークの再構成，サーバーの要塞化（堅牢化）
- 情報セキュリティに関する理解の向上

ネットワークを再構成し，攻撃に強いネットワークにすることは有効な対策である．例えば，DMZ（非武装地帯）と呼ばれるネットワークセグメントを設置し，外部からのアクセスはすべてそのネットワークへと流れるようにすることで，万が一 Web サーバーや DNS サーバーなどが汚染されてしまった場合でも内部ネットワークへの被害を抑えることが可能である．また，通信の暗号化を使用しメールやデータを盗聴から守り，不要なアクセスが行われないような設定にすることも必要である．その他にも，プロキシサーバーを設置する，ネットワークを部門ごとに分離して影響範囲を狭める等が挙げられる．

情報システムに関わる者の情報セキュリティに関する理解の向上も対策として有効である．管理者は新たな脆弱性やソフトウェアアップデートなどの最新の情報を手に入れる必要があり，それを踏まえた上で情報システムの運用をしなければならない．そのため，情報セキュリティに関する知識を得ることや各サーバーの脆弱な点やネットワーク上で攻撃が行われやすいサーバーを知ることは，非常に有効な対策となる．それに加え，事務員や役員など技術者以外の者の理解も重要である．例えば，2011 年の大手重工メーカーに対して行われた標的型攻撃の例 [9] では，情報セキュリティに関する知見を得ることで，初期潜入段階でのマルウェアの侵入を遅らせることが可能であった．万が一初期潜入を許してしまったとしても，その後の内部調査の段階で，ファイルの暗号化やメールの暗号化等を行うことにより窃取される認証情報やデータ等を少なくすることが可能である．攻撃者はソーシャルエンジニアリングなどを利用し接触を試みるため，組織全体の情報セキュリティモラルを向上させることも必要である．

以上のような対策を行う上で共通する重要な点は，双方とも攻撃者の視点を得ることが対策に繋がるという点である．攻撃者の行動や手法を熟知していれば，攻撃に強いネットワーク構成にする，暗号化の重要性やマルウェアの危険性を認識した上でメールをチェックする等，より堅牢な情報システムを構築し利用することが可能になり，標的型攻撃の対策として有効であると考えられる．

攻撃者の視点を対策に活かす例として，専門家に依頼し脆弱性のチェックを行うペネトレーションテストを行う，実際にネットワーク上で演習を行い知見を得るなどといった例が挙げられる．ペネトレーションテストは，ネットワーク上の情報システムが攻撃対象となった場合に，どの程度のセキュリティ侵害が起こるのか，実際に試すことで調査を行う手法である．ペネトレーションテストを行う専門の企業もあり，有効な対策として位置づけられている．実際にネットワーク上で演習を行う方法では，主にセキュリティコンテストやサイバー攻撃を模擬した演習が挙げられる．セキュリティコンテストやサイバー攻撃を模擬した演習等で実際に攻撃，防御を行うことでセキュリティ技術者を強化・育成を行う取り組みが行われている [4]．また，Capture the Flag（CTF）と呼ばれる問題回答形式でのセキュリティ演習や研究も行われている [10]．

2.3 脅威トレース

脅威トレースとは，情報システム上でマルウェアがどのような挙動を取りうるか網羅的に探索し，脆弱性を調査するネットワークシミュレーターであり，現在，研究開発が進められている [6]．脅威トレースは，プログラミング言語 Scala で記述されており，アクターモデルを採用している．各サーバーやアプリケーションを一つのアクターで表し，それぞれのアクター間の通信をメッセージパッシングにより実現しているため，非同期通信による高速な動作が可能である．脅威トレースの特徴はアクターモデルによる網羅的探索が可能な点で，マルウェアの取りうる動作や発生する通信，アプリケーションの動作を分岐させ全ての動作をシミュレートすることにより，脆弱性の調査が可能である (図 1)．

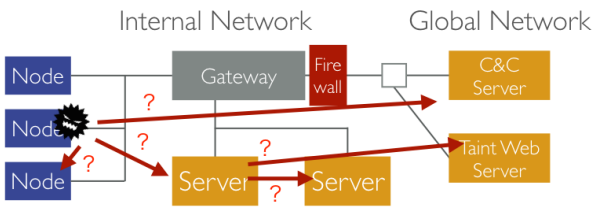

図 1 脅威トレースのイメージ

マルウェアの動作は，Mitre 社が公開している脆弱性情報データベース（Malware Attribute Enumeration and Characterization）[11] や情報セキュリティ企業・機関等が収集したマルウェアに関する情報を分析し，機能ごとに分類したものを抽象化し実装している．標的型攻撃で使用されるマルウェアは主に個別攻撃手法と共通攻撃手法の 2 つの機能を持つ．個別攻撃手法ではその対象に特化した攻撃手法が用いられ，ゼロデイ脆弱性やソフトウェア脆弱性を狙ったエクスプロイトが使用されている．しかし，共通攻撃手法の攻撃方法は既存の攻撃方法等，一般的な攻撃方法が多く，分析をすすめることで攻撃手法の分類を行うことが可能である．

脅威トレースは，ネットワークの機能やマルウェアの動作などの抽象度を高め，一般的な情報システム環境より高いレイヤーでシミュレートを行う．また，マルウェアの機能や標的型攻撃の事例の分析結果を元に，目的の動作を損なわずに抽象化しているため，組合せ爆発やタスクの処理の増大を抑えることが可能である．それに加えて，シナリオベースの実行が可能になっている．シナリオとは，標的型攻撃の事例や想定する攻撃の流れを模したものであり，脅威トレースはそのシナリオに沿って順に実行し，脆弱性の調査が可能である．

3. 攻防戦

3.1 従来の攻防戦

攻撃者の視点を得ることは標的型攻撃の対策に非常に有効である．しかしながら，実際に起こった標的型攻撃の事例から，攻撃者の考えや行動傾向を読み取ることは容易ではない．攻撃者の視点を得るためには，自身が攻撃者となり情報システムを攻撃することが必要である．

しかしながら，実際に企業や組織・個人などに攻撃を行うことは情報セキュリティモラルの観点からも許されることではない．そこで，攻防戦を仮想ネットワーク上で行う大会や，サーバーに対し攻撃を行う演習が世界各地で行われている．

3.2 シナリオベースの攻防戦

サイバー攻撃に限らず，一般的な攻撃への対策として，実際の攻撃を想定したシナリオに沿った演習や訓練を行うことが多々ある．例えば防衛省や自衛隊では，他国からの脅威に対抗するために演習を行うことがあるが，その内容はありとあらゆる状況を演習するのではなく，あるシナリオに基づいて演習が行われることが多い．また，机上演習も行われており，シナリオベースでの演習は非常に重要な対策となっている．

標的型攻撃対策の演習にもシナリオに基づいた演習は非常に重要であり，防衛省のサイバーレンジ演習 [12] でもこの考え方が採用されている．

3.3 攻防戦のメリット

攻防戦のメリットとして，以下の点が挙げられる．

- 標的型攻撃の分析結果からは取得が難しい攻撃者の視点の獲得が可能
- 情報セキュリティや情報技術に関する知識や経験を積むことが可能

攻防戦を行うことで，分析結果などからの取得が難しい，攻撃者の視点を得ることが可能である．攻防戦は，仮想ネットワーク上で情報システムやアプリケーション設定を模して行われ，攻撃側と防御側の役割を担い行われる．攻撃側は，攻撃者の視点から対象ネットワークに対して攻撃を行う．例えば，脆弱のある Web サイトやサービスが存在しており，攻撃側はそのサービスの脆弱性を突いて攻撃を行う．脆弱性を入口にサーバー内部を調査し，サーバー内部で得られた情報を元に接続している別のサーバーに接続し，情報を取得していく．防御側は，プロセスやログを確認し，攻撃されている部分を修正することで脆弱性やサービスの修正を行う．

また，攻防戦を通し知識の再確認や新たな知識の取得を行うことが可能である．これにより，競技者が想定できなかった抜け道や攻撃手法を発見することが可能である．

3.4 従来の攻防戦のデメリット

従来の攻防戦のデメリットとして，以下の点が挙げられる．

- 開催コストが高い
- 複雑な攻防戦となるほど理解が進みにくい
- 競技中に行われた行動の追跡やログの確認が難しい

攻防戦は情報システムに実際に構築し参加者をローカル環境に集めて行われることが多い．例えば SECCON[4] では，運営側が実際のマシンや仮想マシンを使用し脆弱な情報システムを構築する．その後，参加者がローカル環境の閉じたネットワーク上で攻防戦を行う．そのため，運営側と参加者側双方の負担が大きく，開催は容易ではない．特に，競技として攻防戦を行う場合，開催後に同じ情報システムを使用することは出来ないため，コストと取得可能な知識量を比較すると非常に効率が悪いと考えられる．

また，従来のような攻防戦では，攻防戦のレベルが上がるにつれ複雑な攻撃手法や大量の知識が必要であり，攻撃

者の視点を獲得しにくい場合がある．特に，オンサイトで開催されるセキュリティ大会では，攻防戦を競技として捉えられているため，意図して複雑なネットワーク構成や技術を要することが多い．

それに加え，従来の攻防戦では，物理的なネットワークを介して攻防が行われることが多く，パケットのログやアプリケーション・サーバーのログの追跡が非常に難しいというデメリットがある．競技によっては大量のログが記録されることもあるため，それらを追跡することは難しい．万が一不正があった場合に調査を行うことが難しいだけではなく，競技終了後のレビューを難しくするため理解を狭める原因となる．

3.5 従来の攻防戦例

SECCON は特定非営利活動法人日本ネットワークセキュリティ協会 (JNSA) が開催する日本における最大規模のセキュリティ競技大会である．決勝戦では King of the Hill 形式と呼ばれる，運営側が用意したサーバー上でフラグと呼ばれる特定のキーワードを書き込み（攻撃），他のチームからそれを守る（防御）方法で行われる．予選を勝ち抜き，選抜された参加者をローカル環境に集め，運営側がサーバーを用意し行われる．そのため，非常に開催コストが高く，開催が容易ではない．また，攻撃者の視点を得るような問題構成ではなく，技術力を競う大会となっている事が多い．SECCON の地方大会で開催されている「Attack and Defense」では，攻撃側と防御側に分かれ，サーバー上で実際に脆弱なサービスを攻撃・運営する攻防戦が行われている．この大会では，実際の Web サービスやよく使用されるアプリケーションを使用しより現実に近い攻防戦が行われるため，攻撃者の視点を得るには有用な大会である．しかしながら，参加者はローカル環境に集められ，実際の機器やネットワークを構築して行われるため，非常に開催コストが高い．また，大量のログが分散して配置されるため，攻撃のトレースが行いにくいという問題がある．

CRIAB(Cyber-Range-in-a-Box)[5] は，米 Boeing 社が開発しているサイバーセキュリティ演習環境である．不正アクセスや改竄など，様々なセキュリティインシデントに対処する一連の流れ（シナリオ）を演習形式で体験することが可能である．CRIAB は，インシデント対応に重点が置かれており，攻防戦を行うためのツールではないが，ネットワークシミュレータとしての完成度が高いため，攻防戦に有用であると考える．しかしながら，実際の機器を用意する必要があり，非常に高コストである．また，防御面に重点が置かれており，攻撃者の視点を得ることが難しい場合があると考えられる．

4. 脅威トレースの攻防戦化

4.1 利点

脅威トレース上で攻防戦を行う利点として，以下の点が挙げられる．

- 攻防戦開催コストが低い
- シミュレート機能を使用可能
- 抽象度が高く設定されているため，情報セキュリティに疎い技術者でも理解が容易

従来の攻防戦は非常にコストが高く開催が容易ではなかったが，脅威トレースはネットワークやアプリケーションノードが抽象化され，全てソフトウェア上で動作するため，脅威トレースで攻防戦を行う場合，ソフトウェア配布のみで行うことができ，非常に開催コストが低くなる．また，ネットワークモデルを記述することによりカスタマイズ性の高いモデル構成が可能である．修正やアップデートも従来のような実際の端末を使用する場合と比較し，低コストなため，容易であると考えられる．

また，従来の攻防戦は設定した攻防戦シナリオから逸脱するような，予期しない解法が存在する場合が多々ある．そのような抜け道が存在する場合，参加者の理解が進まないだけではなく攻防戦自体が成立しない事も考えられる．脅威トレースを攻防戦化することで，本来の目的である脆弱性調査機能を利用可能であるため，問題シナリオ作成者が意図しない脆弱性（想定外の抜け穴）を調査することが容易である．

従来の攻防戦は，特定のアプリケーションの脆弱性や仕様の穴を利用し，様々な推測と試行の元に攻撃を進める方法が一般的であるが，そのような高度な攻防戦はかえって技術の理解を狭める原因となる場合がある．脅威トレースはその性質上，抽象度が高く設定されており，実際のネットワークやアプリケーション表現を抽象化しているため，情報セキュリティに疎い技術者でも理解が容易な攻防戦が実現可能である．

4.2 実装

脅威トレースの攻防戦化を行う上で，まず攻防戦で必要な機能を分析した．独立行政法人情報処理推進機構（IPA）の作成した分析資料 [1][13] や実際に攻防戦を開催し得られたログ，実際の攻防戦に参加し得られた知見を元に大まかな機能を列挙し，脅威トレースで表現可能な範囲で分類を行った．その結果が以下である．

- サーバー・ノード
  ファイルシステム・シェル・ユーザー
- ネットワーク
- アプリケーション
  マルウェア・サーバークライアントアプリケーション

- ログ
- インターフェース

脅威トレースは以上の機能のうち，サーバー類やアプリケーション類，ネットワーク類の機能はシミュレート可能である．また，マルウェアやログの機能も使用可能であるため，脅威トレース上で攻防戦を行うには，それぞれを使用するためのシェルの機能やユーザーの切り替えなどに加え，ユーザーが使用するインターフェイスを実装する必要がある．そこで本研究では，現在の脅威トレースを拡張し，攻防戦用のサーバープログラムとクライアントプログラム（攻防戦フレームワーク）を作成した．イメージを図 2 に示す．

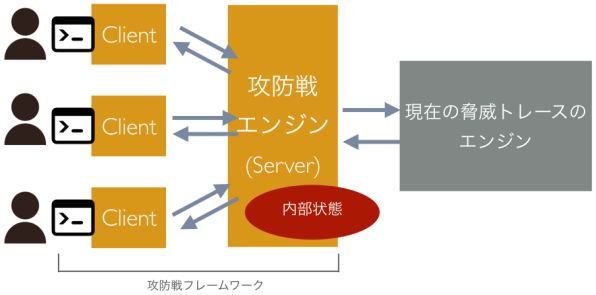

図 2 攻防戦フレームワークのイメージ

4.2.1 プログラム全体

脅威トレース本体にはユーザー判別機能や攻防専用のモデル定義が存在しないため，本体にユーザーを扱える仕組みとモデル定義を付加した．ユーザーはユーザー名・パスワード・ログイン可能/不可能フラグからなるクラスで表し，パスワードはハッシュ値で保存することにより，実際のユーザー定義に近づけている．これにより，パスワードのハッシュ探索などを模擬可能である．また，情報は全て攻防戦フレームワーク本体に格納されている．そのため，すべての操作が攻防戦管理者のもとで行われ，ログのトレースの容易化や不正防止などが可能である．

4.2.2 サーバープログラム

脅威トレースは，メイン関数でネットワークの表示やそれぞれのノードの操作，アプリケーションの操作を行うことが可能である．それぞれのノードやアプリケーションがアクターとして動作し，メッセージパッシングを行うことで通信を模擬している．また，メイン関数内でモデルの定義から実際のアクターの生成が行われている．そこで，メイン関数をアクターとして振る舞う攻防戦サーバープログラムに置き換え，そのサーバープログラム内で攻防戦用のモデル定義からアクターを生成するように改良した．これにより，脅威トレースの機能をそのまま流用し，攻防戦のエンジンとして利用可能にした．

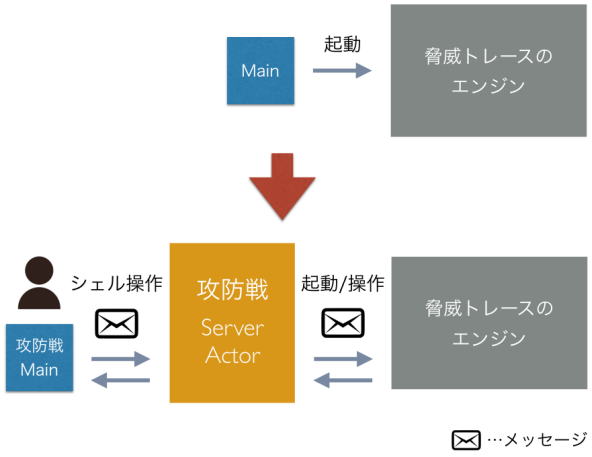

図 3 攻防戦用サーバー

図 3 はサーバープログラムのイメージである．図 3 の上段が従来の脅威トレース，下段が改良後の脅威トレースである．従来の脅威トレースは，メイン関数から脅威トレースのエンジンを直接起動し，ループ中に入出力の送受信を行っていた．改良後は攻防戦のメイン関数から攻防戦サーバーのアクターを生成し，メイン関数内からメッセージパッシングにより攻防戦サーバーアクターとやり取りを行う．攻防戦サーバーアクターでは脅威トレースのエンジンとメッセージパッシングによりやり取りが行われ，ネットワークモデル内の操作が可能である．また，攻防戦サーバーアクターはクライアントアクターからの入力を受け付けることが可能である．

攻防戦サーバーは，内部にプレイヤー情報を保持し，それに応じてノードの切り替えや認証，プレイヤータイプ判別などを行う設計にしている．いずれもメッセージを受け取った後にメッセージの種類（プロトコル）により動作を変えることができ，脅威トレースの起動・停止や初期化処理，クライアントからの構文を解析する等の動作を行っている．上記に加えて，ノードごとに異なるコマンドを使用可能な実装を行った．

4.2.3 クライアントプログラム

クライアントプログラムには，サーバーに接続し入力をサーバーへと渡す機能と，出力を表示する機能を実装した．これらもアクターを使用しており，非同期で処理可能である．以下の図 4 は，そのイメージ図である．

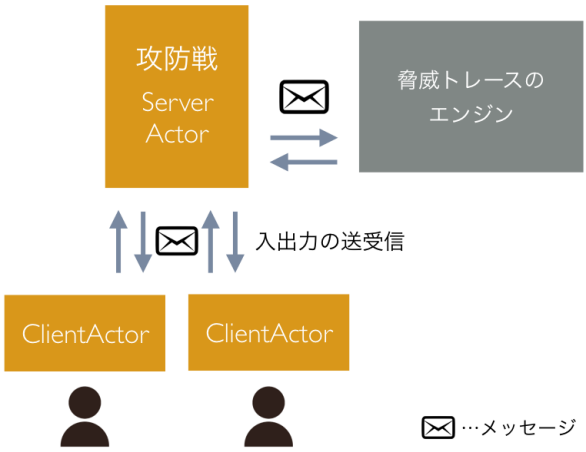

図 4 攻防戦用クライアント

クライアントは，サーバーと接続しメッセージの受け渡しによって入出力を行う．複数のクライアントを起動してサーバーに接続することも可能である．管理者役や攻撃者役のプレイヤーは，このシェルを通じてサーバーと対話を行う．初めに，プレイヤーコードを入力させることで，プレイヤーの判別を行っている．また，サーバーとクライアント間の通信は，クライアントが入力を行うとそれに応じたプロトコルでサーバー側にメッセージが伝えられ，メッセージパッシングにより実現している．

4.2.4 非同期処理

脅威トレースは非同期動作を行うプログラムである．そのため，クライアントからの要求も非同期で処理が行われ，サーバーから送信された出力文字列の受け取りとクライアントの動作続行が重複してしまい，上手く出力ができないという問題があった．そのため，サーバーにログバッファを用意し，クライアントからの要求の処理をバッファに溜め込むことにより，操作上・表示上の問題を解決した．溜め込まれたバッファは，クライアントからの要求で確認することが可能であり，非同期の動作を行う場合も正常に動作させることが可能な設計にした．

4.3 評価

4.3.1 評価手法

実際に発生した標的型攻撃の事例を一つのシナリオとして考え，攻撃側と防御側双方のシナリオを作成し，それらのシナリオを構成する機能が改良後の脅威トレース上で表現可能かどうかを確認することで，攻防戦が実現可能であるかの評価を行った．シナリオベースの演習は標的型攻撃に対して非常に有効な対策であるため，評価としては適切であると考えられる．そこで，2011 年に行われた大手重工メーカーの標的型攻撃のシナリオを使用し，必要な機能の分析を行い，その機能が改良した脅威トレース上で表現可能かどうかを確認した．

4.3.2 評価シナリオ

攻撃側と防御側のシナリオを作成した．以下がそのシナリオである．

攻撃側

(1) C&C サーバーを起点にシェルを操作する
(2) 潜伏させておいたマルウェアに司令を出す
(3) 新しいマルウェアをダウンロードをする
(4) ネットワーク内部へのマルウェアの拡散する
(5) 必要な情報を収集する
(6) C&C サーバーに窃取した情報を送信するれば勝利となる

防御側

(1) ネットワークリストを見ながら，ネットワーク内を探索する
(2) ID・パスワードを使用し，端末に接続する
(3) マルウェアを探す
(4) 削除を試みる
(5) 全てのマルウェアが削除されるまたは C&C サーバーへの接続が遮断されれば勝利となる

以上のシナリオを模擬するためには，以下の表 1 で挙げた項目が必要となる．

表 1 大手重工メーカーへの標的型攻撃機能分類

分類	機能
ネットワーク	データの送受信など
サーバー・ノード	シェル
	ファイルシステム/操作
	アプリケーション実行
	アプリケーションの削除
	ユーザー（認証）
マルウェア	C&C サーバーと接続
	マルウェアの拡散
	ファイルの窃取（送信）
	動作の変更
ログ	ログを確認する
インターフェース	入出力を受け取る
	端末に接続

この機能を模擬可能であるか確認を行った．

4.4 評価結果

4.3.1 節の評価方法に基づき，必要な機能と実装した機能を比較し，実装ができているかの確認を行った．以下の表 2 がまとめた評価結果である．○は実装できている機能，△は実装はできているが動作として不適切な機能，×は実装できていない機能を示している．

表 2 評価結果

分類	機能	実装成否
ネットワーク	ルーター・データの送受信など	○
サーバー・ノード	シェル	○
	ファイルシステム（ファイル操作）	○
	アプリケーション実行	○
	アプリケーションの削除	○
	ユーザー（認証）	○
マルウェア	C&C サーバーと接続	○
	マルウェアの拡散	×
	ファイルの窃取（送信）	○
	動作の変更	○
ログ	ログを確認する	△
インターフェース	入出力を受け取る	○
	端末に接続	○

4.5 考察

概ね表 1 の機能を模擬できていたが，ネットワーク内部へのマルウェアの拡散について実装ができていないという結果になった．これは，現在の脅威トレースの C&C サーバーの実装は一つのマルウェアを操作するものとして作成されており，複数のマルウェアを管理する仕組みが備わっていないためである．しかしながら，現在の C&C サーバーの実装に複数のマルウェアをリストで管理する仕組みを作成する，または，マルウェアの個数分 C&C サーバーを準備することにより模擬可能であると考えられる．また，ログの出力機能については，実際の動作を出力しユーザーに示すことは可能であったが，ログの表示や実装方法に問題があった．ログの表示に関しては，日時が不明な点や閲覧時にログを削除している実装となっている点，ノードやアプリケーション毎にログが保持されるのではなくプレイヤーに紐付けられている点に問題があり，実際のサーバー・アプリケーションのログ機能の動作とは異なる部分がある．これは，実装の段階で標準出力への書き込みの模擬として実装していることに起因する．そのため，ユーザー自身のみ実行ログを確認するシナリオの場合や，標準出力としてログ機能を使用する場合はこのままの実装でもシナリオに沿った攻防戦が可能とであるため，△としている．解決策としてログ情報に日時を付加する，ログ情報をファイルに保存する実装に変更する等が挙げられる．ログ情報は一つのグローバルなオブジェクトに番号付きで格納されているため，十分実装が可能であると考えられる．以上の結果より，脅威トレース上での攻防戦化が実現可能であると考えられる．

5. おわりに

本研究では，脅威トレース上で攻防戦が行えるようにシステムを改良することで，情報システムの設計者や管理者が攻撃者の視点を獲得することを支援した．脅威トレース上での攻防戦は 4.5 節で述べたとおりに可能であると考えられるが，複雑な攻防戦を行うためには更に機能を充実させていく必要がある．例えば，攻撃側の機能として，ファイルを窃取する機能やマルウェアの動作を変更する機能を実装しているが，これに加え，プラグイン形式でマルウェアの動作変更を行う機能や，新たに認証サーバーやデータベースサーバーなどのサーバーアプリケーションを実装することで，より複雑で現実的な攻防戦が行えるようになると考えられる．

謝辞

本研究は独立行政法人情報処理推進機構の支援および，JSPS 科研費 24500043 の助成を受けたものです．

参考文献

[1] 独立行政法人情報処理推進機構（2014）:「『高度標的型攻撃』対策に向けたシステム設計ガイド」, p.2.(オンライン), 入手先 〈https://www.ipa.go.jp/files/000046236.pdf〉,（参照 2016-01-29）
[2] 二木 真明，佐藤 元彦，山崎 文明，内田 勝也 (2012),「標的型サイバー攻撃と APT に関する考察」, 2012-CSEC-56 巻，20 号，p1 － 8
[3] 日経 BP 社 (2014) ,『「攻撃者」の視点で考えるサイバー攻撃対策』，杉浦隆幸，「日経コンピュータ」，p96-99
[4] SECCON: 〈http://www.seccon.jp/〉,（参照 2016-01-29）
[5] Boeing,「Cyber-Range-in-a-Box」 , 〈http://www.boeing.com/defense/cybersecurity-information-management/〉,（参照 2016-02-03）
[6] Kato, M. Matsunami, T. Kanaoka, A. Koide, H. and Okamoto, E. : Tracing Attacks on Advanced Persistent Threat in Networked Systems, In Proc. SafeConfig 2012 5th Symposium on Configuration Analytics and Automation (October 2012).
[7] Scala, 〈http://www.scala-lang.org/〉,（参照 2016-02-03）
[8] 警察庁（2015）,「平成 26 年中のサイバー空間をめぐる脅威の情勢について」, p.1.(オンライン), 入手先 〈https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf〉,（参照 2016-01-29）
[9] 独立行政法人情報処理推進機構（2012),「標的型サイバー攻撃の事例分析と対策レポート」, p.3.(オンライン), 入手先 〈https://www.ipa.go.jp/files/000024536.pdf〉,（参照 2016-01-29）
[10] James Walden :A real-time information warfare exercise on a virtual network,SIGCSE '05 Proceedings of the 36th SIGCSE technical symposium on Computer science education, Pages 86-90, (2005)
[11] Mitre 社,「Malware Attribute Enumeration and Characterization」, 〈https://maec.mitre.org/〉,（参照 2016-01-29）
[12] 加賀智也，佐野裕香，城間晴輝，小森旭，亀田健一，坂下圭一,「サイバー攻撃対処に関する研究」, 入手先 〈http://www.mod.go.jp/atla/ats2015/image/pdf/1-11.pdf〉,（参照 2016-01-29）
[13] 独立行政法人情報処理推進機構（2014）,「新しいタイプの攻撃」の対策に向けた設計・運用ガイド，入手先 〈https://www.ipa.go.jp/files/000017308.pdf〉,（参照 2016-02-04）