「マルチメディア，分散，協調とモバイル
(DICOMO2017)シンポジウム」 平成29年6月

サイバー攻撃対策のための人工知能搭載型サイバーレンジの検討

大石恵輔[1] 中山能之[1] 岩東佑季[1] 石川博也[1] 宮本貴義[2] 八槇博史[2]

概要： 標的型攻撃では，ネットワークに侵入したマルウェアが各ホストをネットワークの内部から攻撃する．この動作を仮想計算機と SDN を用いて構成したサイバーレンジを用いてシミュレーションする．このサイバーレンジでは，攻撃側と防御側の双方に人工知能が搭載され，これらの人工知能を遺伝的アルゴリズム等により進化させることで，将来発生しうるサイバー攻撃の予測に繋げることを本研究では企図している．仮想ネットワークシステムの構築のためにネットワーク記述言語 NSDL を定義し，サイバーレンジにおける各種の動作を制御するための API 機構，および人工知能を進化させるための共進化シミュレーション機構や，ＡＩによるサイバー攻撃をサイバーレンジ内で実現するための攻撃プランナーといったモジュールを開発した．

Cyber Range Equipped with Artificial Intelligence for Cyber-Attack Experiments

KEISUKE OISHI[1] YOSHIYUKI NAKAYAMA[1] YUKI IWATO[1]
HIROYA ISHIKAWA[1] TAKAYOSHI MIYAMOTO[2] HIROFUMI YAMAKI[2]

1. はじめに

近年，標的型攻撃の増加により，LAN 内からもサイバー攻撃が来ることが予想される．LAN 内に侵入されたとき，どの様な攻撃があるのか，どの様な攻撃パターンがあるのかが問題である．また，マルウェアにも AI 機能が組み込まれた攻撃も予想され具体的にどの様なことが起きるのか検討を行う必要がある[1].

検討を行うために我々はクラウド上に複数の仮想マシンと仮想ブリッジを用いた仮想ネットワークシステムと監視システムから成るサイバーレンジと，攻撃から学習する防御システムおよび攻撃を学習する攻撃システムから成る人工知能を合わせた人工知能搭載型サイバーレンジの検討を行った．

2. 人工知能搭載型サイバーレンジ

人工知能搭載型サイバーレンジとは，図 1 に示すサイバーレンジと人工知能から構成される．

サイバーレンジに AI 機能を搭載することにより 2 つのことが可能になる．1 つ目は攻撃を模擬して人工知能を用いたサイバー攻撃対策システムの防御訓練に用いる事が出来る．人工知能搭載型サイバーレンジからサイバー攻撃対策システムに攻撃を行い，攻撃から得られる事象を元にルールを作成し，ルールを元に防御するという対策に用いる．攻撃手法の学習を行う対策方法でこのような流れでルールを作成するが，AI を用いる事によって将来起こりうる攻撃を模擬してやることでそこで起きた事象をもちいて攻撃手法を学習することが考えられる．2 つ目は将来，AI を用いた攻撃の出現が予測される．その時攻撃者側は何を学習してくるのか模擬することが可能となる．

そこで我々は両者が学習する環境のシミュレーションを行うことで，共進化に基づく攻撃と防御の予測を提唱してきた[2].

サイバーレンジと人工知能を統合することにより防御側 AI と攻撃側 AI がサイバー攻撃を模擬することによって，攻撃を受けることにより将来起こりうる事態を予測と，攻撃側の将来的な攻撃を AI により模擬することが可能になる．

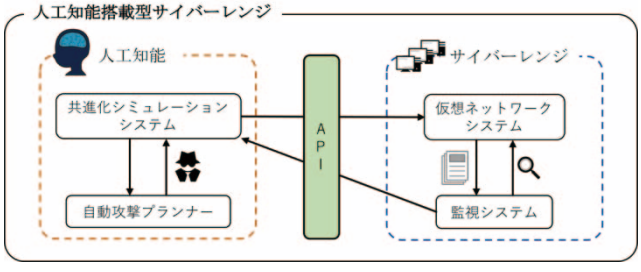

図 1. 人工知能搭載型サイバーレンジ

3. サイバーレンジ

サイバーレンジとはサイバー空間で行われるサイバー

1 東京電機大学情報環境学研究科 印西市
2 東京電機大学情報環境学部 印西市

攻撃模擬し演習や訓練を行うものである[3].

例えば，攻撃対象のネットワークが仮想空間に用意され，サイバー攻撃を行い，陥落させるスピードを競い合うものや，各チームに分かれ自チームの脆弱なサーバーを守りつつも相手チームの脆弱なサーバーに攻撃を仕掛け合いながら長時間サービスを稼働できたチームが勝者といった訓練がある．

サイバーレンジを用いる事により物理的な機器を用意することなく仮想的に構築できることや，実際に使用している環境を模擬してやることで，本番環境同じ環境で演習することが利点としてあげられる．

サイバーレンジのシステムとして，仮想ネットワークシステム，制御を行うための API，監視システム 3 つで構成される．

3.1 仮想ネットワークシステム

サイバー攻撃を模擬するためのネットワーク環境として仮想ネットワークシステムの開発を行ってきた[4]．複数の仮想マシンと仮想ブリッジから構成される仮想ネットワーク，ネットワーク構造の記述から仮想ネットワークの自動構築をする 2 つの機能がある．

仮想ネットワークとは実在する LAN をソフトウェア上で仮想定期に実行する物であり，仮想環境で行う事によって同時並行での検証が可能になる．

シミュレーションを行うに当たって仮想ネットワークシステムを変化させ自動構築を行う機能が必要になる．ネットワーク記述言語（Network Description Language，以下 NDL）はアムステルダム大学の J.J van der Ham らがネットワークのシンプルかつ明確な記述が可能である言語として考案を行った．しかしながら，具体的な文法，記述例などは発表されて折らず基本概念のみである．

そこで我々は記述言語としてネットワークシミュレータ記述言語（Network Simulator Description Language，以下 NSDL）を定義した．NSDL はネットワーク構造，仮想マシン，ネットワーク機器などをシミュレーション環境に構築するために必要である論理構成を記述するために，要素をコンマ区切りで記述しコンピュータ可読な形式として記述を行う．この NSDL を用いて仮想ネットワーク構造の記述を行うことによってソフトウェア上での構築が容易になることや，記述を変更することによって多様なネットワークにも対応することが可能になる．

NSDL の文法について説明をする．NSDL は json 形式で表現され，大きく分けて，各ノード情報，コンテナ名を指定する“name”，インタフェース関連を記述する“if”，ルーティングを行う“fwd”，ブリッジを記述する“br”，コンテナイメージの存在を記述する“image”の 6 つの要素か構成される．

各ノード情報には端末名，ルータ，仮想マシン等の端末の種類が記述される．論理接続に関する情報については，今回構成を行うに当たって L2 スイッチを中心とし結線を行うと想定したため，接続先である L2 スイッチの記述を行う．IP 層に関する情報では，結線を行った後 IP 層での通信を可能にするために，IP アドレス，ネットマスク，デフォルトゲートウェイの記述を行う．ルーティングを行う“fwd”には行き先，ネットマスク，出力先を記述する．ブリッジを記述“br”には作成する仮想スイッチ名を記述する．コンテナイメージの存在を記述する“image”にはイメージ名，イメージの作成に必要な Dockerfile の場所を記述する．記述例を図 2 に示す．

```
"top": [
  {
    "name": "top",
    "if": [
      {
        "if_name": "if1",
        "connect_br": "br1",
        "ipaddress": "10.0.0.1/8"
      },
      {
        "if_name": "if2",
        "connect_br": "br2",
        "ipaddress": "59.31.1.1/24"
      }
    ],
    "fwd": [
      {
       "destination": "10.7.0.0/16",
       "genmask": "255.255.255.0",
       "gw": "10.0.0.2"
      },
      {
       "destination": "10.7.0.16/30",
       "genmask": "255.255.255.0",
       "gw": "59.31.1.2"
      },
      {
       "destination": "10.1.1.0/24",
       "genmask": "255.255.255.0",
       "gw": "10.0.0.2"
      }
    ]
  }
"br": [
  {
    "br_name": "br1"
  }
],
"images": [
  {
    "name": "mail",
    "Dfile": "mail"
  }
]
```

図 2．NSDL による記述例（一部を抜粋）

3.2 API

仮想ネットワークシステムの拡張性を高めるため API の開発を行った．このことにより後述する共進化シミュレーションシステムとの連携することが可能となり，利便性の向上と効率化を図った．

システム構成に当たって，WEB サーバーには API に対するアクセスが多いことや，Docker 本体に影響を与えないことなどを考慮し，並行処理に優れ，メモリ使用量が少ない Nginx を採用した．また，ウェブアプリケーション開発フレームワークには既存コードの活用や軽量，高速である点を評価し，オープンソースである Python で記述された Pyramid を用いた．データベースシステムには Pyramid で

標準利用される SQLite を用いている．システムの構成を図 3 に示す．

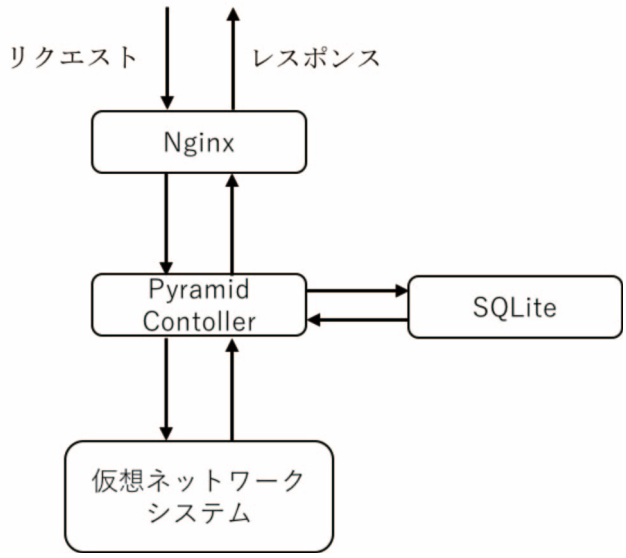

図 3．API 概要図

リクエストを Nginx で受け取り，Pyramid のコントローラーが仮想ネットワークシステムに対して構築等の処理を行い，Nginx を通じて Pyramid のコントローラーは処理結果を返却する REST API である．

3.3 監視システム

仮想ネットワークシステムで攻撃と防御のそれぞれの有効性の検証を実現するために必要となるネットワークの自動監視システムの開発を行った[5]．求められる機能として，ネットワーク環境内に存在するホストの自動登録，監視項目の設定や対象ホスト毎に監視結果の取得機能が必要である．開発時点で，仮想ネットワークシステムで使用できる攻撃監視専用の監視ツールがないため既存の監視ツールを用いて開発を行った．

ラトビアで開発が行われている Zabbix SAI が開発するオープンソースの統合監視ツール Zabbix を採用した．Zabbix では監視設定のバリエーションやサーバーや OS ごとに用意されている監視項目をまとめたテンプレートが豊富に提供されている．その一方で，テンプレートの適用，新たな監視設定の追加や監視結果であるデータ収集などについては Web ブラウザ上から手動操作することが前提とされているため監視システムとして用いるために自動操作機能を別途用意する必要がある．

テンプレートの適用，新たな監視設定の自動追加するための解決策として Zabbix API の itemCreate 関数を使用したプログラムを実装した．引数として関し項目名，監視するファイルパス，監視の際に使用するキーワードおよびテンプレートの id を与える．これによって手動での監視項目の設定をすることなくプログラムによって自動的に登録される．

監視結果の自動取得の問題を解決するため Zabbix API の historyGet 関数を使用したプログラムの実装を行った．引数として監視対象のホスト id および，そのホストに適用されている監視項目の id を与える必要がある．これによって Web ブラウザでの監視結果を確認せずにデータを取得することが可能になった．

最後に監視対象のホスト毎に監視データの収集を行うに解決策として Zabbix に登録済みのホストの一覧を json 形式で取得し，これを元にホスト毎のデータ格納ディレクトリを作成，監視項目の id 一覧を該当ディレクトリに保存するプログラムを実装したこれによってホスト毎に収集したデータの格納を実現した．

4. 人工知能搭載型サイバーレンジ

サイバーレンジで守る防御側 AI である共進化シミュレーションシステムと攻撃を行う攻撃側 AI である攻撃プランナーをあわせて人工知能搭載型と呼ぶこれら 2 つについて説明を行う．

4.1 共進化シミュレーションシステム

近年マルウェアの急速な増加の背景としてマルウェア生成ツールキットによって手軽に多様な組合せのマルウェアが可能になっていることやマルウェアの亜種が大量に発生している．新たな対策が講じられるとそれに対応して新たな手法が生まれるといったイタチごっこが続いている．これに対抗するために防御側も共進化計算を利用して攻撃側の変化に対応するようなモデル化し，シミュレーションすることによってサイバー攻撃の予測や防御の対応策を検討するシステムである．我々はそのアプローチの 1 つとして共進化モデルに基づく出現の予測を目指している．

我々はシミュレーションの大量平行実行を実現するクラウド上のシミュレーションプラットフォーム GPGCloud を開発してきた．本システムは組合せを効率よく探索する物であり，Amazon Web Services のクラウド上に構築した．シミュレーション機構の概要を図 4 に示す．

Manager は最初に実行するパラメータセット群を生成する．初期パラメータセット群を生成後，生成した各パラメータセットをクラウド上の仮想計算機に渡し，対象モデルのシミュレータを用いて実行する．実行結果は次世代の生成に必要になるため，Manager へ返される．Manager では，実行したパラメータセットが有用であるかをスコア関数により評価し，その評価を基に，次に実行するパラメータセットを生成する．生成された次世代の各パラメータセットは初期終段と同様にクラウド上の仮想計算機に渡されたのち，シミュレータを用いて実行される．このシミュレーション機構ではパラメータ探索を行うメタアルゴリズムとして遺伝的アルゴリズム（GA）が実装されており，パラメータを大量に生成し，有用なパラメータセットを効率よく探索するという機能を持っている．また，クラウド上に構築

することによってスケールアウトが容易であり，VM を大量に生成し，シミュレーションを並行実行することで効率の良いシミュレーションが可能である．

人工知能搭載型サイバーレンジと使用する想定として，VM 上にて仮想ネットワークシステムを実行し，Manager は API を経由してパラメータセットや実行結果のやりとりを行う．

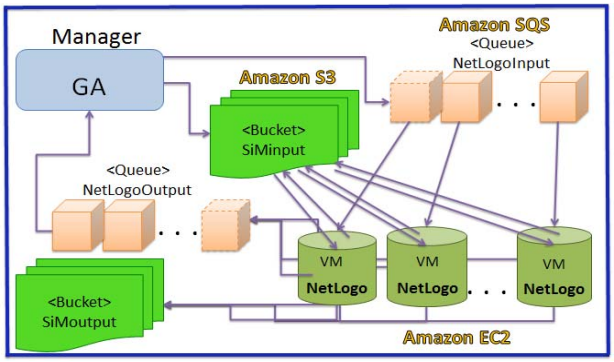

図 4．共進化シミュレーションシステムの概要図

4.2 攻撃プランナー

攻撃プランナーは，攻撃者が AI 機能を搭載したマルウェアを社内サーバーに侵入させた場合を仮定して，目的の攻撃行為を達成するまでの攻撃プランを人工知能の一分野であるプランニングを用いて自動生成を行うものである．

現在のサイバー攻撃に用いられる一般的なマルウェアは，感染したサーバーから C&C（Command and Control）サーバーへ通信を行い，外部から指令を受け取りつつ感染を LAN 内部の機器へと感染を拡大していく．しかし将来的には，C&C サーバーにアクセスすることなく，AI を搭載したマルウェア単体でサーバー侵入し，攻撃者からの指示を一切受けずに侵入したマルウェア同士で自律する自律型マルウェアを模擬することによって攻撃経路を導き出す事が可能である．

5. プロトタイプ

共進化シミュレーションシステムを用いて日本年金機構情報流出事件が起きたネットワーク構成を最低限模擬したサイバーレンジの作成を行った．作成したネットワークを図 5 に示す．点線で囲ったルータ，ブリッジ，クライアントから構成されるサイバーレンジを仮想計算機上に構築を行った．

6. おわりに

我々は今後マルウェアにも AI 機能が組み込まれるという予想のもと今後具体的にどの様な事が起きるのか検討を行うためにクラウド上に複数の仮想マシンと仮想ブリッジを用いた仮想ネットワークシステムと監視システムから成るサイバーレンジと，攻撃から学習する防御システムおよび

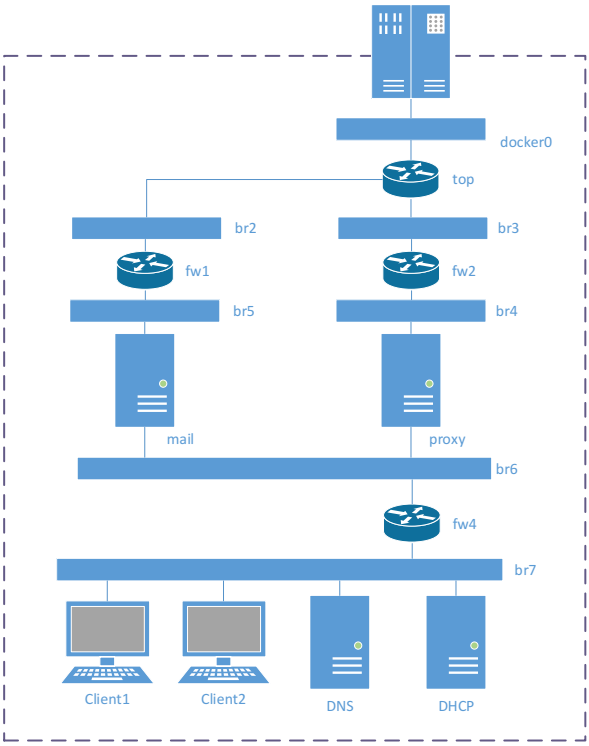

図 5．仮想計算機に構築したサイバーレンジの例

攻撃を学習する攻撃システムから成る人工知能を合わせた人工知能搭載型サイバーレンジの検討を行い，今後どの様な事態が起きるのかを具体的にシミュレーションを行い，検討を行うことが可能となった．今後，これらのシステムを用いて実際のネットワークシステムを模したシミュレーション実験を行い，サイバー攻撃の将来予測へとつなげていく方針である．

謝辞

本研究は JSPS 科研費 16K12439 の助成を受けたものです．

参考文献

[1] 八槇博史“人工知能技術を用いた標的型サイバー攻撃に関する一考察”，2016 年 電子情報通信学会総合大会，DS-2-2，2016.

[2] 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”，2016 年 電子情報通信学会総合大会，DS-2-2，2016.

[3] Bernard “Chip” Ferguson, Anne Tall, “National Cyber Range Overview”, 2014 IEEE Military Communications Conference, 2014.

[4] 大石恵輔，八槇博史，“サイバー攻撃実験のための仮想ネットワーク自動構成方式の検討”，2016 年 電子情報通信学会総合大会，DS-2-4，2016.

[5] 中山能之，八槇博史，“仮想ネットワークシステムにおける自動攻撃と監視システムの実装”，2016 年 電子情報通信学会総合大会，DS-2-5，2016.