4W-04

標的型攻撃の体験ができる自習型演習システムの提案と実装

八代 哲† 宮田 大地‡ 馬場 隆彰‡ 細井 理央‡ 角田 裕太‡
渡辺 亮平‡ 高橋 和司‡ 細谷 竜平† 齋藤 孝道†
明治大学† 明治大学大学院‡

1.はじめに

組織における機密情報の窃取などを目的とした攻撃の一つに，標的型攻撃[1]がある．その中でも，メールを契機とした標的型攻撃（以降，標的型メール攻撃と呼ぶ）の報告件数が増加している[2]．そのメールは，攻撃者が攻撃対象の組織の構成員に対して送信し，受信者の端末で，攻撃者が準備したマルウエアを実行させることを目的としたものである．

標的型メール攻撃による被害が増加している原因の一つに，標的型攻撃自体の認知度が低いことが挙げられる．IPA の報告[3]によると，標的型攻撃及びその脅威を知らないと答えた回答者は，全体の 48.8%であった．よって，標的型攻撃の対策として，標的型攻撃の全体像を体験的に学習することが重要だと考えられる．

そこで本論文では，標的型メール攻撃の体験演習ができるシステムの提案及び実装を行う．提案システムを用いた演習により，NCWF[4]，SecBoK[5]でのシステムとアプリケーションのセキュリティ上の脅威と脆弱性に関する知識を身につけることを目指す．本論文では，提案システムの演習の効果を，受講者のアンケートにより評価する．

2.提案システム

提案システムは，サイバーレンジ及び演習支援システムによりクラウド上に構成される．本論文において，提案システムの受講者は，演習支援システムの指示により演習の進め方を確認し，その後サイバーレンジ上の各インスタンスを用いて演習を行う．

2.1. サイバーレンジ

一般にサイバーレンジとは，サイバー空間上で行われる演習及びその環境を指す[6]．提案システムにおけるサイバーレンジは，VMware vSphere Hypervisor[7]を用いて実現されているので，受講者は各インスタンスの操作が容易であり，演習をスムーズに行える．

A Proposal and Implementation of Training System for Self-Studying Targeted Attacks
†Satoshi YASHIRO ‡Daichi MIYATA ‡Takaaki BABA
‡Rio HOSOI ‡Yuta TSUNODA ‡Ryohei WATANABE
‡Kazushi TAKAHASHI †Ryohei HOSOYA
†Takamichi SAITO
†Meiji University ‡Graduate School of Meiji University

2.2. サイバーレンジのシステム構成

サイバーレンジのシステム構成を図 1 に示す．図 1 に書かれている用語及び各インスタンスの概要は以下の通りである．

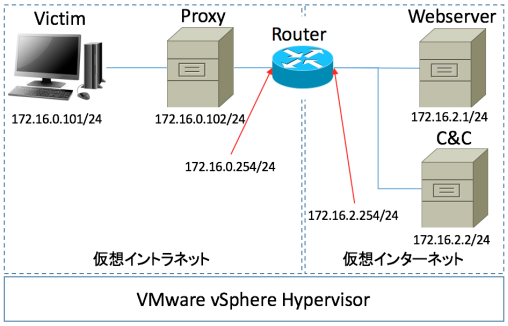

図 1　サイバーレンジのシステム構成

- 仮想イントラネット
  仮想的に構築した企業内ネットワーク．
- 仮想インターネット
  仮想的インターネットを疑似するネットワーク．
- Victim
  標的型メール攻撃演習（後述）において，被害を受ける端末．
- Proxy
  Victim から送信されたパケットを中継するプロキシサーバ．被害端末を特定する演習（後述）で，受講者は Proxy のアクセスログを調査する．
- Router
  仮想イントラネットと仮想インターネットを分割するルータ．ファイアウォールが設定されている．
- Webserver
  攻撃者が標的型メール攻撃を行う際に必要となるマルウエアを仕掛けた Web サイト．
- C&C（Command & Control）
  標的型メール攻撃演習（後述）で，攻撃者が使用する攻撃用ツールがインストールされている端末．

2.3. 演習支援システム

演習支援システムは Moodle により実現される．Moodle[8]とは，オープンソースの e ラーニング

プラットフォームである．演習支援システムには，各演習の概要及び手順が書かれているので，受講者は演習支援システムの表示を見ながら，演習を自習形式で進められる．また，演習支援システムには演習問題が書かれているので，受講者はそれに解答することで演習に対する理解度を確かめられる．

3.演習内容

提案システムを用いて体験できる二つの演習の概要を述べる．

3.1. 標的型メール攻撃演習

この演習は，受講者が攻撃を仕掛ける側（以降，攻撃演習者と呼ぶ）と，被害を受ける側（以降，被害演習者と呼ぶ）の２つの役割に分かれて，標的型メール攻撃を体験できる演習である．攻撃演習者は C&C を操作し，被害演習者は Victim を操作する．本演習では，Victim がマルウエアに感染し，その後攻撃演習者が Victim の画面のスクリーンショットを窃取する流れを体験演習できる．

本演習の流れは，以下の通りである．

1. 攻撃演習者は，C&C にインストールされている攻撃ツールを起動し攻撃の準備をする．
2. 被害演習者は，受信した設定の Victim の画面上に表示されている標的型攻撃メールの本文のリンクをクリックする．ここで，Victim のデスクトップには機密情報があるとする．
3. Victim は Webserver にアクセスする．
4. Victim がマルウエアに感染し，C&C との通信を始める．
5. 攻撃ツールは Victim の画面のスクリーンショットを自動で撮影する．
6. 攻撃演習者は，5. で撮影された Victim の画面のスクリーンショットから機密情報を窃取する．

3.2. 被害端末を特定する演習

この演習は，受講者がプロキシサーバのアクセスログ（以降，ログと呼ぶ）により，標的型メール攻撃の被害端末の IP アドレスを特定する演習である．本演習に先駆け，受講者はログの見方及びログの調査において利用できる UNIX コマンドを，演習支援システムで学習できる．本演習において受講者は，Proxy のログを，less コマンド及び grep コマンドを用いて調査する．その結果，標的型メール攻撃が発生した際に，プロキシサーバに残るログの特徴を理解できる．

4.評価

提案システムが，標的型攻撃の認知度の向上に貢献しているかを評価する．明治大学理工学部情報科学科に在籍する学部三年生及び四年生 22 名に，3 節に示した二つの演習を受けてもらい，演習後に以下の A，B に示すアンケートを取った．いずれも，1 から 10 の整数で回答してもらった．数値が大きいほど，理解度が高いとする．回答の平均値を算出した結果を表 1 に示す．

A) 演習前と演習後で，標的型攻撃の全体像についてどの程度理解しているか（したか）

B) 演習前と演習後で，標的型攻撃の脅威についてどの程度理解しているか（したか）

表 1 アンケートの結果

	演習前	演習後
A	4.45	7.14
B	4.95	8.40

アンケートの結果から，提案システムでの演習を受けた受講者の，標的型攻撃に対する認知度が向上したことが分かった．

5.まとめ

本論文では，標的型メール攻撃の体験演習ができる自習型演習システムの提案と実装を行った．また，提案システムの評価を行い，提案システムが，標的型メール攻撃の理解の向上に貢献していることを示した．

6.参考文献

[1] “標的型攻撃/新しいタイプの攻撃の実態と対策” https://www.ipa.go.jp/files/000024542.pdf
[2] “平成27年におけるサイバー空間をめぐる脅威の情勢について” https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf
[3] “2015年度 情報セキュリティの脅威に対する意識調査 - 調査報告書 -” https://www.ipa.go.jp/files/000050002.pdf
[4] “DRAFT National Cybersecurity Workforce Framework” http://csrc.nist.gov/nice/framework/DraftNationalCybersecurityWorkforceFrameworkV2.xlsx
[5] “セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版 全体整理表” http://www.jnsa.org/result/2016/skillmap/data/skillmap-secboK2016.xlsx
[6] “情報セキュリティの現状と動向について -サイバー演習の実施要領と演習事例-” https://ssl.bsk-z.or.jp/kakusyu/pdf/27-1jyouhousekyurithityousakennkyuu.pdf
[7] http://www.vmware.com/jp/products/vsphere-hypervisor.html
[8] https://moodle.org/?lang=ja