標的型攻撃に対するセキュリティ教育を自動化する訓練システムの開発

塩田 智基，北原美里，山下大貴，喜田 弘司

香川大学

s16t233@stu.kagawa-u.ac.jp

Development of Automatic Training System for Security Education Against APT

Tomoki Shiota，Misato Kitahara，Daiki Yamashita，Koji Kida

Kagawa Univ.

概要

近年標的型攻撃に対するセキュリティ教育は緊急課題と言える。2018 年の時点では 6000 件以上の被害が発生したという調査結果も挙げられている。標的型攻撃は急激な速度で広まっており、セキュリティソフトだけでは、対策しきれない背景がある。しかし、現在のセキュリティ教育は教材を作るコストが高い、講義を行う頻度が多いため教育を行うコストが高いといった課題がある。本稿ではそれらの課題を解決する、標的型攻撃に対するセキュリティ教育を自動化する訓練システムの開発を行った。本訓練システムでは、教育を自動で行い教育コストを下げる効果が期待できる。また、本研究は標的型攻撃の中でも標的型攻撃メールを対象に行っている。

1 はじめに

近年標的型攻撃の被害が拡大しており、2018 年の時点では 6000 件以上の被害が発生している[1]。現在の標的型攻撃の対策は大きく 2 つあり (1) セキュリティソフトによる対策、(2) セキュリティ教育により各個人の情報リテラシーを向上させ標的型攻撃の被害を防ぐというものがある。特に近年の標的型攻撃はセキュリティソフトのみでは対応することが難しく、より一層セキュリティ教育の重要性は高まっていると言える。

そこで本研究では、標的型攻撃に対するセキュリティ教育を自動化する訓練システムを提案し、実際に開発を行う。

2 課題

セキュリティ教育には、教師側と受講者側という立場が存在する。以下それぞれの立場で課題の分析を行う。

2.1 教師側の課題の分析

教師側は受講者側に標的型攻撃に対する教育を行う。主な役割として(1)教材を作成、(2)講義の実施がある。これら(1)(2)に関して、企業などの組織で行う社員教育(倫理教育等)と標的型攻撃の教育の特性の違いは以下の通りである。

(1)に関しては、社員教育の教材は教育内容の変化が少ないため、教材を作り直す必要はない。一方で標的型攻撃の教材は、最新の攻撃に追従する必要があり、随時教材を作り直す必要がある。これは教師への負担が大きくなることが課題である。

(2)に関しては、社員教育の場合前回行った教育内容を忘れさせないための復習がほとんどであり、年度替わりなどの固定のタイミングで年に 1 回程度の頻度で行えばよい。一方で標的型攻撃に対する教育は、常に攻撃が進化するのでそれに対応するため、攻撃の流行が変わるタイミングで教育を実施する必要がある。

2.2 受講者側の課題の分析

受講者側は教師が用意した教材で標的型攻撃に対する教育を受ける。受講者側で重要となる観点は(1)教育効果が高い教育、(2)教育効果の維持がある。これら(1)(2)に関して、企業などの組織で行う社員教育(倫理教育等)と標的型攻撃の教育の特性の違いは以下の通りである。(1)に関しては、

社員教育の場合では、Web 教材などを利用した座学でも十分な効果が得られる。一方で標的型攻撃の教育に関しては、座学による教育では十分な教育効果が得られない場合がある。例えば、実際に攻撃を受けた場合対処できないことが多く、より実践的な教育が必要である。(2)に関しては、社員教育の場合では、身に付けるべきことが変わらないため教材も変化することが少ない。従って、忘れた頃に復習をするだけで十分である。一方で標的型攻撃の教育は、攻撃の流行が変わる度に教材が変化する。従って、教材が変わる度に教育を受けないと効果が維持できない。

2.3 課題のまとめ

現在のセキュリティ教育は、攻撃の例を Web 教材で提示して注意喚起を行うのが一般的である。標的型攻撃は日々進化するため従来手法では以下の課題がある。

課題 1: 最新の標的型攻撃に追従した教材を人が作るためコストが高い

課題 2: 定期的に講義を受けなければ最新の標的型攻撃に対応することが難しい

さらに、Web 教材を利用した教育の他に、訓練システムを用いた教育方法も存在するが、大多数が手動で訓練を実施しているため、現状の標的型攻撃に対する訓練システムには以下の課題がある。

課題 3: 継続して訓練を行うことが難しい

これらの課題を克服することが標的型攻撃の対策として重要なものになると考えている。

3 コンセプト

現状の標的型攻撃に対するセキュリティ教育の課題を解決するシステムとして、標的型攻撃に対するセキュリティ教育を自動化する訓練システムを提案する。本研究は標的型攻撃の中でも標的型攻撃メールを対象に行っている。この訓練システムは日常的に行っているメール処理に訓練メールを紛れさせ、その訓練メールで行われた処理を解析し、その解析結果を利用して教育を行う。

3.1 導入イメージ

訓練システムの導入イメージを図 1 に示す。図 1 では、利用者、教師、メールシステム、訓練システムから構成される。ここで言う利用者は、受講者のことである。メールシステムは利用者が日常的に利用するメールの送受信をするサーバである。提案システムは以下の 3 つの役割がある。(1)メールシステムから利用者の受信メールを受け取り、訓練メールを生成する。(2)メールシステムを介して訓練メールを利用者に送信する。(3)利用者が訓練メールに対して行った処理を解析し、利用者にその結果を提示する。また提案システムは、利用者に案内メールを送信することで解析結果を確認させるように促す。

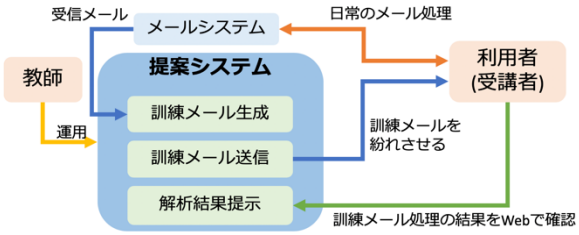

図 1 本システムのコンセプト

3.2 課題の解決

課題 1 は、標的型攻撃で使われるメールを受講者の受信メールをもとに自動生成することで教材を作る必要がなくなり解決する。課題 2、課題 3 については、受講者が日常的に行っているメール処理の中で、訓練を行わせることで講義形式の教育を行う必要がなくなり解決する。

3.3 訓練の流れ

訓練システムを利用した訓練の実施方法について述べる。利用者は日常的にメール処理を行っていると仮定する。図 2 に訓練の実施方法の流れを示す。図 2 は、利用者と訓練システムのやり取りをフローチャートで表したものである。訓練の流れは以下の通りである。

① 利用者は本システムに登録する。

② 訓練システムから訓練メールが送信されるので、利用者はその訓練メールを処理する。

③ 訓練システムは利用者が訓練メールに行った処理を解析し、利用者はその解析結果を確認し学習を行う。

利用者は②と③を常に繰り返し続けることで訓練を行う。

システム内では訓練を行うために必要な処理が各行程間で行われている。①と②間では、利用者

の受信メールを解析し訓練メールを生成する。また、訓練メールに添付するファイルの生成も行う。生成した訓練メールを利用者に送信する。②と③間では、利用者が訓練メールに行った処理を解析しその結果を提示する。また同じタイミングで新たな訓練メールの生成を行う。

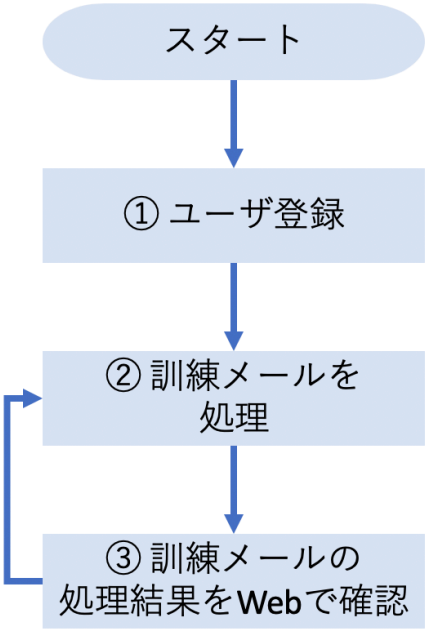

図 2 訓練の流れ

3.4 教師側の振る舞いの変化

本システムを導入することで、教材の自動生成、日々のメール処理の中で訓練を行えるようになる。そのため、講義を行う必要がなくなり、教師側の課題であった、教材を作成するコストが高い、定期的に講義を行う手間の 2 点を解決することができる。また、本システムはメールの解析結果を可視化するページを用意しており、教師側は本システムを使った利用者の監視が行えるようになり、個別に効果的な教育を実施する時間を設けやすくなると考えている。可視化したページの例を図 3、図 4 に示す。図 3 は、横軸が日時、縦軸が数となっており、送信された訓練メールの数、訓練メールの既読数、訓練メールに添付されたファイルの実行数、訓練メールに添付された URL の実行数毎に折れ線グラフで表したものである。図 4 は、送信された訓練メールの数、訓練メールの既読数、訓練メールに添付されたファイルの実行数、訓練メールに添付された URL の実行数が示されている。

なお、図 4 のページは教師側のみ確認することが可能であり、利用者には別で解析結果を確認するページを用意している。

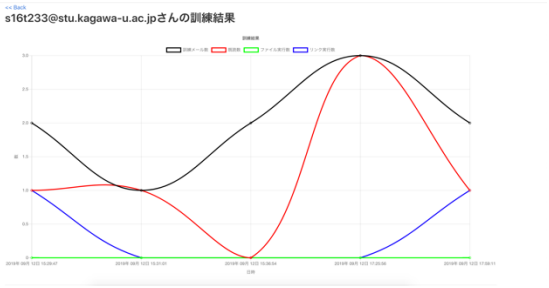

図 3 メール処理を解析したグラフ

図 4 利用者の訓練結果(管理者用)

3.5 利用者側の振る舞いの変化

本システムを導入することで、日々のメール処理とそのメール処理の解析結果をシステムで確認する行為が、講義による教育の代わりとなるので利用者側の課題であった、定期的に講義を受けるコストが高い、実践的に教育を継続して受けるこ

が難しいという 2 点の課題を解決することができる。図 5 に解析結果のページを示す。図 5 では、図 4 の内容と同じものであるが、1 日分のデータしか表示されていないという違いがある。これは、利用者側は最新の解析結果を確認するだけで教育内容を知ることができる。そのため、一度にすべての解析結果を確認する必要がない。なお、過去の解析結果も確認することはできるようにしている。

図 5 利用者の訓練結果(利用者用)

4 提案システム

提案システムの機能、及びその機能の処理について述べる。本システムは企業や教育機関などの組織単位で利用してもらうことを想定しているため、教師側がシステムを運用する必要がある。そこで、教師側の負担を低くするためにシステムの運用コストを下げる必要があり、その実現方法について述べる。最後に実装に利用した技術を述べる。

4.1 システムの試作

本システムの基本機能は以下の 2 つである。

訓練メールの自動生成機能: 利用者が普段受信するメールに似せた、訓練メールを生成する。

訓練結果提示機能: 利用者が訓練メールに対して行った処理から騙された回数などの訓練結果を提示する。

これら機能を実現するシステム構成図を図 6 に示す。システムで行われる処理は 3 つのフローを非同期に並列して動作する。

訓練メール生成処理: メールサーバから利用者のメールデータを取得する(①)。解析部でこのデータをもとに、利用者が普段受信するような訓練メールを自動生成する。自動生成された訓練メールはインタフェースを介して DB1 に保存する(②)。

訓練メール送信処理: インタフェース部で不定期に DB1 から訓練メールを取得し、利用者に送信する(③)。利用者は受信したメールを処理する。訓練メールの添付ファイルの実行はインタフェースを介して DB2 に保存する。

訓練メール解析処理: 定期的にメールサーバからメールを取得し訓練メールの開封結果を取得し(④)、DB2から添付ファイルの実行結果・訓練メール内のリンクの実行結果を、インタフェースを介して取得する(⑤)。これらのデータから騙された回数等を、インタフェースを介して DB3に保存する(⑥)。DB3の結果を利用者に提示する(⑦)。

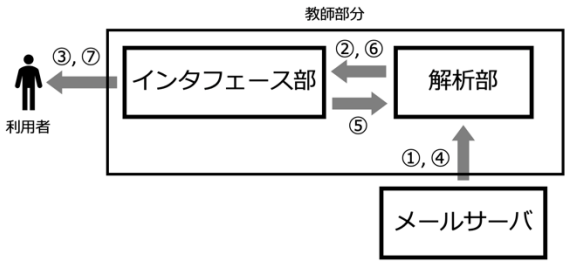

図 6 システムの構成図

4.2 運用コストを下げる方法

本システムは基本的にすべて自動で動作するため、インタフェースに何かしらのイベントを与え続けなければならない。そのため、インタフェースを監視するためのツールを用意する必要がある。監視方法として監視ツールがインタフェース側に実装した REST API に等間隔にリクエストを送信し続けるポーリング処理で監視を行う。ソケット通信を採用していない理由としてインタフェース部を冗長化し、Web サーバでロード・バランシングした際、コネクションを何度も繋ぎ直す手間がなくなるからである。また、システムの可用性の向上を図るために、ジョブ実行機能や、本番環境ではロード・バランサを導入し、負荷分散を行う。

4.4 システムの実装技術

本システムはインタフェース部、解析部、監視部に分けて実装する。

基盤技術として Docker を用いる。Docker のコンテナ管理には Docker Compose を用いる。

インタフェース部では Ruby on Rails を用いて Web アプリケーションとして実装を行う。
Ruby on Rails を選択した理由として、基本機能にメーラー機能、ジョブ実行機能、ストレージ機能などが存在しているためである。また、開発速度を重視した結果この技術を選定する事とした。
DB には MySQL、セッション・ジョブ監視には Redis を用いる。

解析部は、インタフェース部から Docker コンテナを経由してプログラムを呼び出すため、ほぼすべてのプログラミング言語で実装可能である。現在は Ruby、Python3、Node.js、Java、C#などで実装を行っているが、状況に応じてプログラミング言語を使い分けて開発していく。

監視部は、インタフェース部を等間隔で監視する必要性があるため、非同期処理が得意な Node.js を用いて実装する。
また、本システムの実運用時にはロード・バランサによるスケーリングを想定しているため、Web サーバに Nginx を採用する。

5 今後の課題

今後の課題として検証があげられる。本システムの検証は 2 度行う。1 回目の検証では、訓練メールの自動生成は行わず教師が登録した訓練メールのみで訓練を行う。この検証は、訓練形式の教育を継続して行った場合の効果を確認するために行う。教師側の課題と利用者側の課題が解決できているかはアンケートを利用して確認する。2 回目の検証では、訓練メールの自動生成を行うようにし訓練を行う。この検証では、メールの自動生成を導入した場合でもシステムが効果的に動作しているか確認する。

本システムは先行研究である[2]の研究をベースに開発を進めている。よって、1 回目の検証結果としては[2]のような効果が得られると考えている。

最終的には、訓練メール自動生成機能を使って自動で効果的な教育が行える訓練システムを目指す。

6 おわりに

本稿では、標的型攻撃に対するセキュリティ教育を自動化する訓練システムの開発について述べた。本システムは教材を自動生成し教育を日常のメール処理に紛れさせて行うものである。検証時には継続して訓練が行えることとメールの自動生成が意味を成しているかを検証するため、2 度に分けて検証を行う。

参考文献

[1] 警察庁、 平成 30 年におけるサイバー空間をめぐる脅威の情勢等について、https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf 、2018 年 3 月 7 日

[2] 太田祐平、辻由紀、相良智則、照井健良、染谷由美子、西田一雄、加藤恒生、情報セキュリティ意識向上への取り組み ～標的型攻撃メールを想定した防災訓練の実施、日本血液事業学会 第 41 巻、第 3 号、p761-767、2018 年 11 月

[3] 米谷雄介、後藤田中、小野滋己、青木有香、宮﨑凌大、八重樫理人、藤本憲市、林敏浩、今井慈郎、最所圭三、香川大学での標的型攻撃メール訓練の導入と改善点の検討、学術情報処理研究 22 巻、第 1 号、p54-63、2018 年 9 月