キャンパスネットワークにおけるインシデント対応の自動化 – シミュレーション実験の報告 –

佐藤 聡 [1)], 三宮 秀次 [1)], 片岸 一起 [1)], 中井 央 [1)], 亀山 啓輔 [1)]

1) 筑波大学 学術情報メディアセンター

akira@cc.tsukuba.ac.jp

Automation of incident response in campus network – Report of simulation experiment –

Akira Sato [1)], Shuji Sannomiya [1)], Kazuki Katagishi [1)], Hisashi Nakai [1)], Keisuke Kameyama[1)]

1) Academic Computing & Communications Center, University of Tsukuba

概要

我々は管理者によるインシデント対応のコストを軽減するためにインシデント対応の自動化の手法を 2018 年度 AXIES 年次大会のポスターにて提案している。本論文では、提案手法により管理者のコストがどの程度軽減できるかを、筑波大学の無線 LAN システムのファイアウォールログを用いてシミュレーションした結果について報告する。

1 はじめに

大学においても、セキュリティの維持管理は重要な課題の一つである [1][2]。セキュリティを維持するために、次世代型ファイアウォール等の不正侵入検知装置・不正侵入防御装置（以下 IDS と呼ぶ）を用いて、セキュリティ的脅威のある通信を遮断することを可能としている。一方、遮断しても、セキュリティ的脅威を取り除いているわけではない。大学のネットワークは限られた人員で管理運用しており、これらを取り除く作業を完璧に行うことは難しい。

我々は、文献 [3] にて、管理者による管理コストを軽減するために、インシデント対応を自動化する方法についての考察を行なった。この方法では、セキュリティ的脅威が発生した時に自動的にネットワーク利用を制限することにより、利用者本人が利用しているコンピュータを特定し、インシデントの対処をする方法である。しかし、ネットワーク管理者の作業量が、この方法によりがどの程度軽減されるかは未検証であった。そこで、現在運用しているネットワークの記録をもとに、この方法を用いることでどの程度管理作業が軽減されるかのシミュレーションを行った。この論文ではその結果を報告する。

2 提案手法

本手法では、利用者を以下の 4 つのレベルの重要度に分ける。

レベル 0 「初期状態」を表す。何もイベントが発生していない状態。セキュリティ的な問題がない状態。（問題があるかどうかわからない状態も含まれる。）

レベル 1 「注視状態」を表す。何らかのイベントが発生したが、今すぐに当該コンピュータ調査する必要なない、あるいは調査する必要がないと判断される状態。例えば、不審サイトへの接続が確認されたものの、その接続が不正侵入防御装置によって遮断されている場合などがあげられる。すなわち、新たに問題のあるイベントが発生しないか注視しておく状態である。

レベル 2 「制限状態」を表す。何らかのイベントが発生したが、今すぐに対応すべきではないが被害拡散の予防のため、通信制限をかける状態。通信制限の例として、セキュリティアップデートのための通信等以外は禁止するなどが考えられる。

レベル 3 「禁止状態」を表す。何らかのイベントが発生し、直ぐに対応が必要なため、ネットワークの利用を禁止する状態。

本手法では、セキュリティ維持を行う装置の各種ログ出力や、脆弱性検査の結果、キャンパスネットワーク外部・内部からのインシデント報告等をインシデントに関するイベントと定義する。このイベントには、実際にインシデントが発生している場合のものだけではなく、インシデントを未然に防いだ場合のものも含まれる。イベントは、その内容に応じて、あらかじめ、以下に示す 3 種類に分類しておく。それぞれの種類ごとで管理対象をどのレベルに移動させるかを決めておくことにより、インシデントの重要度を自動的に定めることができる。

注視イベント　レベル 1 未満であれば、レベル 1 にアップさせるイベント。セキュリティ的な問題がないイベント。例えば、不正侵入防御装置によりフィッシングサイトへのアクセスを阻止した場合などが相当する。

制限イベント　レベル 2 未満であれば、レベル 2 にアップさせるイベント。何らかの対応が必要なイベント。例えば、不正侵入検知装置により、マルウェアのダウンロードが確認された場合などが相当する。

禁止イベント　レベル 3 未満であれば、レベル 3 にアップさせるイベント。緊急的な対応が必要なイベント。例えば、不正侵入検知装置により、外部へのサイトの攻撃が確認された場合などが相当する。

3　実験に用いたログデータを取得した環境

シミュレーションを行うためのデータを取得した環境は、筑波大学にて運用を行なっている認証付き無線 LAN システム（以後、無線 LAN システムと呼ぶ）のためのファイアウォールのログを用いた。この無線 LAN システムは、筑波大学の教職員と学生（以後、構成員とよぶ）が利用可能となっている。この無線 LAN システムとキャンパスネットワークとの接続点には Palo alto Networks 社製のファイアウォールが設置されている。このファイアウォールでは、外部からの無線 LAN システムのセグメントへの通信は全て拒否しており、無線 LAN システムのセグメントから外部への通信は原則として全て許可している。また、無線 LAN システムのセグメントから外部への通信に対して IDS 機能を有効にしているため、無線 LAN システムに接続した利用者の端末が発生させたセキュリティ的脅威となる通信はファイアウォールにて遮断している。構成員は利用する機器をこの無線　LAN システムに接続する際に ID を用いて認証を行う。ファイアウォールのログには通信を行なった構成員の ID が記録されている。

表 1　シミュレーションに用いたログの概要

項目	値
期間中に 1 度でも利用した利用者	13242
critical 以上のログを出力した利用者	8
high 以上のログを出力した利用者	29
medium 以上のログを出力した利用者数	1332
critical 以上のログ数	67
high 以上のログ数	648
medium 以上のログ数	21598

シミュレーションを行うデータは、無線 LAN システムのファイアウォールが出力した、2019 年度の長期休暇期間を含まないとある 1 ヶ月のログの中から重大度 (Severity) が critical, high, medium となっているログを抽出したものを用いた。シミュレーションに用いたデータの概要を表 1 に示す。

4　シュミレーション方法と結果

提案手法を以下のように簡素化してシミュレーションすることにした。

1. イベントとしては、ファイアウォールが出力したセキュリティ脅威のログのみと取り扱うことにする。
2. 重大度 (Severity) が medium 以上のセキュリティ的脅威により遮断したというログを、制限イベントとした。すなわち、通信制限が行われたものとする。
3. レベル 3 の状態でレベル 2 に変更する申請（以下、制限解除の申請と呼ぶ）を行うまでの時間を 1 時間、6 時間、12 時間、24 時間の 4 種類にてシミュレーションを行う。制限解除申請の直後にレベル 2 に遷移し、通信制限は解除されるものとした。ここでは、上記 2. の通信が発生した時刻に通信制限が行われるため、その時刻から制限解除申請が行われる時刻までの当該利用者の脅威ログはなかったものとして取り扱う。

それぞれの利用者が通信制限された回数を計測する。具体的には、利用者ごとに上記 2. の制限イベントとなるログの出力回数を計測する。利用者ごとの通

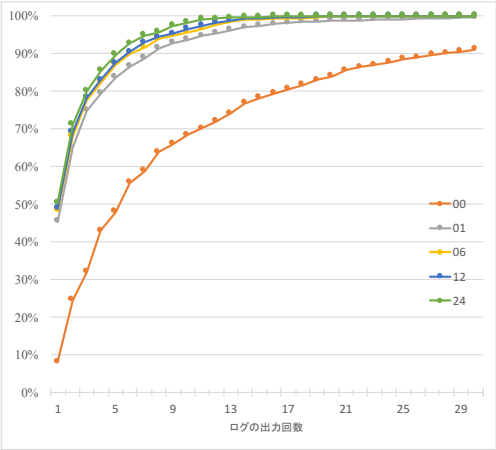

図 1　利用者の累積度数分布

信制限を受けた回数を横軸にした利用者数の累積度数分布図を作成した (図 1)。

図 1 中の 00 のグラフは、比較対象として、上記シミュレーションを行わず、利用者ごとの重大度 (Severity) が medium 以上のセキュリティ的脅威を発生させた回数を横軸とした場合の利用者数の累積度数分布を表している。01, 06, 12, 24 のグラフはそれぞれ制限解除の申請がなされるまでの時間が、1 時間、6 時間、12 時間、24 時間としてシミュレーションした結果を表している。

図 1 中の 00 のグラフより、1 ヶ月の間で、制限イベントとなるログを 1 回だけしか出力してない利用者は、その月に 1 回以上制限イベントとなるログを出力した人の約 8% しかいないことがわかる。

図 1 からわかるように、制限解除の申請までの時間が 1 時間の場合でも、通信制限を受ける回数が 1 回だけであった人は、通信制限を受けた人の約 48% となっている。また、通信制限を受けた人の約 93 % の人は、通信制限の回数が 9 回未満となっている。

制限解除の申請までの時間を増やしたとしても、傾向は大きく変わるとはなく、度数が若干大きくなる程度であった。

すなわち、10 回の通信制限を受けると、管理人による対策が必要とするならば、1 ヶ月で約 84 人の対応が必要なる。このシミュレーションでは、通信制限を受けたとしても何も対応しないで解除申請をした場合を想定しているが、実際には、利用者が何らかの対応をすることが考えられるために実際に対応する人数はこれよりも少なくなることが予想される。

5　まとめ

本論文では、筑波大学の無線 LAN システムのファイアウォールログを用いて、我々が提案した手法に関するシミュレーションを行った。具体的には、重大度が midium 以上のセキュリティ的脅威のある通信を発生させた場合に、すぐに通信制限を行うと、ネットワーク管理者の管理コストが軽減されるかどうかのシミュレーションを行なった。調査対象としたとある 1 ヶ月間に 1 度でも重大度が midium 以上のセキュリティ的脅威のある通信を発生させた利用者は 1332 名であった。制限解除の申請を 1 時間後に行なった場合で、かつ制限を 10 回行うと管理者が対応するというシミュレーションを行なった場合、対応すべき利用者数は 84 人となった。

今後の課題としては、提案手法を実装し、運用してみることである。

謝辞

分析用のログデータを提供いただいた学術情報メディアセンターに感謝する。

参考文献

[1] 岩井亮太, 渡邉英伸, 相原玲二, 近堂徹, 西村浩二, セキュリティ維持活動の情報を活用するインシデント対応進捗管理システム, 情報処理学会研究報告, 2019-IOT-47(4), pp.1-7, 2018.

[2] 森健人, 石井将大, 松浦知史, 金勇, 北口喜明, 友石正彦, セキュリティ事案における知見の蓄積・活用を可能とする対応フローの提案と実装, 情報処理学会研究報告, 2019-IOT-46(2), pp.1-8, 2019.

[3] 佐藤聡, 三宮秀次, 片岸一起, 亀山啓輔, キャンパスネットワークにおける自主的かつ分散的セキュリティ維持管理方式の考察, ポスター発表, AXIES2018.