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

佐藤 聡 [1)], 三宮 秀次 [1)], 片岸一起 [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

A consideration on voluntary basis and distributed security maintenance management method for campus network system

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

1) Academic Computing & Communications Center, University of Tsukuba

概要

現在の日本の大学では、セキュリティの維持管理は重要な課題の一つであるが、それらを任される部門のマンパワーが不足しているため、それらの作業を中央集権的に行うことは大変難しい。本論文では、キャンパスネットワークのセキュリテイ維持管理を自主的、かつ、分散的な方法にて行うことを提案する。具体的には、セキュリティ維持管理の対象を 4 つのレベルにより分類する。インシデントの発生を防ぐ機能や発見する機能からのイベントにより、管理対象のレベルを遷移させる。それぞれのレベルにおいて、誰がどのような対処をするかをあらかじめ決めておく。

1　背景

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。セキュリティを維持するために、インシデントの発生を未然に防ぐための機能や、インシデントの発生を発見する機能などを有する各種の仕組みをキャンパスのネットワークに導入する大学も増えてきている。例えば、ワクチンソフトのようなセキュリティ対策ソフトや、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、脆弱性検査装置などはそれらの仕組みの一部である。これらの装置を有効に活用することにより、大部分のセキュリティの脅威を防ぐことが可能となる [1, 2]。

一方、大学では、キャンパスネットワークに接続される情報機器を統一化することによる情報維持管理コストを下げることは一般的には難しい。事務組織では、業務で利用するソフトウェアを統一することが可能な場合があるが、教員が研究用途で購入する情報機器については研究の自由度を維持するために統一的なソフトウェアの利用といった制約を課すことはできない場合もある。ましてや、学生については、学生自身の教育を受けやすくするために自分自身が購入した情報機器をキャンパスに持ち込んで接続することを許可せざるを得ず、それらの情報機器についての制約を課すことが難しい。

このように、セキュリティの維持管理の対象となる情報機器の数は構成員数を越える数になっている。それに対して、構成員数よりも遥かに少ない教育用端末の管理を行なっている情報センターのような部門が、大学全体のセキュリティの維持管理も担当している場合が多い。すなわち、対応する機器が増えているにもかかわらず、人員を増やすことができない場合も多く、多くの大学ではセキュリティ維持管理を行うマンパワーが不足している。さらに、情報機器数が増えたことにより、インシデント発生件数も増加しており、それらの対応に多くのマンパワーが消費されている。

2　問題点

以上のことより、大学の情報セキュリティ管理部門がセキュリティ維持を行うために、様々な効率化を行なっているが、以下のような問題点がある。

- セキュリティ対策ソフト、侵入検知装置、脆弱性検査装置等のセキュリティを維持する装置により、インシデント発生を未然に防ぐことや、インシデントの発生を予見できることがあり、それらを利用者に通知することにより利用者のセキュリ

ティ維持に関する意識を高めることができるが、そのような事例に対応する余裕がない。

- 利用されるオペレーティングシステム・ソフトウェアの種類が多いため、個々のオペレーティングシステム・ソフトウェアについてのセキュリティ維持のための設定変更や、マルウェアの駆除、再インストールなどの技術的サポートを行うことには限界がある。

3 解決手法

本考察では、上記のような問題を解決する方法として、自主的、かつ、分散的なセキュリティ維持管理方法の提案を行う。以下に、提案方法の大まかな方針を示す。

- 大学全体のセキュリティ維持管理を行う体制を階層的に構築する。具体的には、階層構造の末端としてキャンパスネットワークに接続する情報機器の利用者、中間層としてそれら利用者の所属する組織のセキュリティ担当者、上位層として大学全体を管理するセキュリティ管理部門とする。
- 前述の階層構造において、下位層では対応が難しい場合には、上位層が対応を支援する体制を確立する。
- インシデントに関連するイベントが発生した場合には、トリアージのようにインシデントの重要度を判定する。具体的には、利用者個人で対応可能か、所属組織のセキュリティ担当者が担当すべきかを、セキュリティ管理部門が判断する。
- セキュリティを維持する装置によって防御・予見検知、もしくは発生検知をしたイベントについては、原則としてそのイベントを起こした情報機器の利用者に、その詳細情報を開示して通知する。

セキュリティ維持管理方式の対象は、IP アドレスとそれが使用された時刻の組み合わせから、その IP アドレスの利用者が判別できる IP アドレスを対象とする。静的に IP アドレスの割り当てが行われているサブネットワークの場合、利用者が台帳等により特定できる場合などが該当する。DHCP により動的に IP アドレスの割り当てが行われていているサブネットワークの場合、認証システムや、MAC アドレスの事前登録等により、利用者が特定できる場合などが該当する。

また、重要度の判定のために、対象となる情報機器を、クライアント用途か、サーバ用途かにあらかじめ分類しておく。クライアント用途の機器については、IP アドレスではなく利用者を単位として重要度判定を行う。サーバ用途の機器については、IP アドレスを単位として重要度判定を行う。

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。

本手法では、管理対象を以下の 4 つのレベルの重要度に分けることを提案する。

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、今すぐに対応すべきではない、あるいは対応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。

レベル 1 以上のレベルにレベルアップした場合には、利用者に通知を行い、レベル 2 以上にアップした場合は、必要な対処を促す。レベル 1 になった場合は、利用者に特に対処を求めないが、利用者自身が確認して何らかの事実が判明した場合には報告するように指示する。レベル 1 にて、一定期間イベントがなかった場合にはレベル 0 にダウンする。レベル 2 になった場合は、利用者自身による対処を求める。対処の内容は発生したイベントにより異なるため、対処すべき内容についても指示する。利用者からの対処完了の報告をもって、レベル 1 にダウンさせる。レベル 3

になった場合は、所属組織のセキュリティ担当者による対処を求める。対処の内容は発生したイベントにより異なるため、対処すべき内容についても指示する。所属組織のセキュリティ担当者からの対処完了の報告をもって、レベル 1 にダウンさせる。

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。

この分類を基本として、例えば、同じ種類のイベントが一定時間以内に一定回数以上発生する場合や、一定期間内に同じレベルに何度も遷移する場合、あらかじめ当該情報機器が機微情報を保存していることがわかっている場合などに、重要度 (レベル) 毎の対処内容を変化させるルールを設定可能とする。これにより、きめ細かい重要度 (レベル) の設定を可能となる。

4　今後の課題

現在、我々は、この管理方法に基づいて、認証システムとの連携、IP アドレスの管理システムとの連携、イベントのハンドリング (セキュリティ対策ソフト、不正侵入検知装置・不正侵入防御装置のログ出力との連携や、脆弱性検査装置の結果と連携)、レベルのアップ・ダウンの実装（ファイアウォール装置でのルールの追加方法)、利用者ごとのレベルの管理、利用者への通知、各種情報の開示を行うためのシステムの設計、および、試作を行なっている。

参考文献

[1] Ohmori,Higashino and Kawato,“On a Finite State Machine and Input Fields for Incident Tracking System”, 研究報告インターネットと運用技術（IOT）,Vol.2018-IOT-42,No.6,pp.1-5,2018.

[2] 葛西 真寿, 小倉 広実, 須藤 勝弘, 竹内 淑怜, 次世代ファイアウォールと接続情報検索システム「ヒロミル」によるインシデント・レディネス体制の改善, 第 21 回学術情報処理研究集会発表論文集, pp.63-68,2017.