次世代ファイアウォールの Daily Reports を利用した手作りインシデント・レディネス体制と見えてきた課題

葛西 真寿 1),2), 小倉 広実 3), 須藤 勝弘 3), 竹内 淑怜 3)

1) 弘前大学 大学院理工学研究科

2) 弘前大学 総合情報処理センター

3) 弘前大学 附属図書館事務部

cnc-director@hirosaki-u.ac.jp

Incident Readiness Operation with Daily Reports from the Next-Generation Firewall

Masumi Kasai1),2), Hiromi Ogura3), Katsuhiro Suto3), Sumire Takeuchi3)

1) Graduate School of Science and Technology, Hirosaki Univ.

2) Computing and Networking Center, Hirosaki Univ.

3) Hirosaki University Library

概要

本学における次世代ファイアウォールの Daily Reports をトリガーとしたインシデント対応体制の運用に関し，次に掲げるいくつかの改善を行った．一つ目は次世代ファイアウォールの監視設定の見直しである．二つ目は Daily Reports 内容のカスタマイズである．三つ目は Daily Reports にリストアップされた IP アドレスから実際の利用者を特定するための検索システム（愛称「ヒロミル」）の学内開発である．本稿では，カスタマイズされた Daily Reports をトリガーとし，「ヒロミル」を活用した本学の手作りインシデント・レディネス体制と，その運用から見えてきた課題について報告する．

1　はじめに

昨年度から開始した本学における次世代ファイアウォールの運用体制の概要は，次世代ファイアウォール (Palo Alto Networks 社 PA-5050，以下 PA-5050) が脅威と判断した通信を遮断する機能を利用してセキュリティを確保しながら，遮断しなかった不審な通信については，PA-5050 から毎日送信される Daily Palo Alto Networks Reports (以下，Daily Reports) に基づいて調査を行うというものである [1].

本年度からは，PA-5050 からの Daily Reports による調査を弘前大学 CSIRT の担当業務とし，その際，より迅速なインシデント・レスポンス (事後対処) とインシデント・レディネス (事前対処) 体制の整備を目指し，以下に掲げるいくつかの改善を行った [2].

本稿では，この改善されたインシデント・レディネス体制の運用を通して見えてきた，本学におけるいくつかの課題について報告する．

2　インシデント・レディネス体制の改善

本年度，より迅速なインシデント・レスポンス (事後対処) とインシデント・レディネス (事前対処) 体制の整備を目指して行った改善点は以下の通りである．

2.1　PA-5050 の監視設定の強化

PA-5050 は，それぞれの「脅威/コンテンツ名」(Threat/Content Name) を「重大度」(Severity) による格付をしている．「重大度」は上位から critical, high, medium, low, informational の順である．

当初，デフォルトの状態で PA-5050 を運用していたが,「重大度」が medium や low であっても通信を遮断する一方,「重大度」最上位の critical と判断された脅威であっても通信を遮断せず警告のみのケースがあった．

そこで,「重大度」 critical と判定された脅威については，学外から学内へと学内から学外への双方向を問答無用で遮断（drop）するという設定を行い，数ヶ月の運用後,「重大度」high 及び medium についても

critical に準じて遮断（reset-both）する設定とした．

2.2　Daily Reports のカスタマイズ

次に行ったのは，PA-5050 からの Daily Reports の見直しである．運用当初は 29 ページの PDF で毎日 CSIRT メーリングリストに配信されたが，本年 3 月に総合情報処理センター専任担当教員が転出後，補充人事がペンディングとなってしまったため，センター長である（情報分野の専門家ではない）第一著者自身がこの業務を担当することになったという学内事情もあり，Daily Reports の内容を真に必要なもののみに限定し，見やすいものにするというカスタマイズを断行することとなった．

何回かの試行錯誤の後，当初 29 ページあった Daily Reports は本稿執筆時点で以下の 8 ページである．

カスタマイズして運用中の日報 8 ページの内容

p.1 スパイウェアに感染したと判断された学内ホスト（「アクション」が alert で遮断されなかったもの）

p.2 スパイウェアに感染した上位リストにはリストアップされているが，「アクション」が block-ip, drop, reset-both 等で通信が遮断されている学内ホスト

p.3 上位のスパイウェア脅威と判断された学内ホスト（「アクション」が alert で遮断されなかったもの）

p.4 スパイウェア脅威の上位リストにはリストアップされているが，「アクション」が block-ip, drop, reset-both 等で通信が遮断されている学内ホスト

p.5 ウイルスに感染したと判断された学内ホスト（「アクション」が alert で遮断されなかったもの）

p.6 ウイルス感染の上位リストにはリストアップされているが，「アクション」が block-ip, drop, reset-both 等で通信が遮断されている学内ホスト

p,7 上位の攻撃者にリストアップされている学内ホスト

p.8 上位の被害者にリストアップされている学内ホスト

2.3　接続情報検索システム「ヒロミル」の開発

有線 LAN 及び無線 LAN 接続において全学 DHCP サービスが標準となっている本学において，Daily Reports にリストアップされた IP アドレスから当該利用者を特定するためには，過去の特定の日時に特定の IP アドレスを利用していた接続機器の利用者情報を検索するシステムが必要となる．

その目的のために今回学内開発したこの「**弘前大学キャンパス情報ネットワーク接続機器・利用者情報統合検索システム**」には，開発者（小倉広実）の名前にちなみ，また弘前大学内の接続機器情報を見るという意味も込めて「**ヒロミル**」という愛称がつけられた．「ヒロミル」を利用することによって，当該機器が有線 LAN 接続か無線 LAN 接続かを問わず，わずか数クリックで機器の利用者情報を得ることができるようになり，より迅速なとインシデント・レディネス（事前対処）体制を整備することが可能となった．

3　見えてきた課題

上に述べたように改善された本学のインシデント・レディネス体制を数ヶ月にわたって運用してきた結果，以下のような課題が見えてきた．

3.1　留学生のパソコンに関する脅威対応

まず，外国人留学生が自国語版 OS のパソコンを無線 LAN 接続していて不審な通信が Daily Reports で報告された場合，自国版のウイルス対策ソフトがインストールされていると，部局担当者がパソコン画面から正しくウイルスが駆除されていることを確認するのが困難なことがある．また，パソコン本体にインストール不要の USB メモリ型のウイルス対策ソフトをセンターで用意しているが，これが日本語版 OS にしか対応しておらず，外国語版 OS 上のウイルス対策に有効かどうか確認がとれない．実際に試したところ，USB メモリ型のウイルス対策ソフトの指示通り不審と思われるファイルを削除して行った結果，外国語版 OS が起動しなくなり，再インストールが必要となったケースもある．

各国語版 OS 対応の USB メモリ型のウイルス対策ソフトが望まれる．

3.2　個人で契約した外部メールサービスからのダウンロード

本学が契約しているメールサービス（Office 365）以外の，個人で契約した外部メールサーバからウイルス付きメールを pop3 等でダウンロードしようとして PA-5050 が検知しているケースも複数発見されている．その場合，学内にダウンロードする前に，外部メールサーバ上でできるウイルス対策サービスについて検討するよう依頼したり，真に業務上必要とするものでない限り，個人で契約した外部メールサービスを学内からは利用しないように依頼するなどの対策が考えられている．

3.3　研究室等で独自に設置した無線 LAN ルータ

Daily Reports にリストアップされた，不審な通信を行っている機器が，研究室等で独自に設置した無線

LAN ルータであるケースも複数例あった．特に，無線LAN ルータが NAT モードの場合，CSIRT/センターでは当該事案の利用者を特定できないため，無線 LAN ルータの設定責任者に当該日時に接続していた可能性のある全てのユーザに確認依頼していただくが，場合によっては 10 名以上の利用者にすの都度確認が必要なケースもある．

対策として，研究室等で独自に無線 LAN ルータを設置し，複数の利用者が接続して利用する場合は，ブリッジモードに設定する，またはセンターが動作確認を行った IEEE802.1X 認証対応の推奨機器を購入し，認証の設定を行って使用するなどが考えられている．

参考文献

[1] 佐藤友暁, 須藤勝弘, 小倉広実, 竹内淑怜, 葛西真寿, “MAC アドレス認証システムを用いた次世代ファイアウォールの運用体制構築”, 第 20 回学術情報処理研究集会 発表論文集, pp.43-46, 2016.

[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.