弘前大学 CSIRT の活動実績報告
– 次世代ファイアウォールと「ヒロミル」によるインシデント事前対処 –

総合情報処理センター長　葛西 真寿
附属図書館情報基盤グループ　小倉 広実
須藤 勝弘
竹内 淑怜
{cnc-director, ogura, stowe, s_take}@hirosaki-u.ac.jp

1　はじめに

本稿では、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」を活用した弘前大学 CSIRT の活動について述べる。昨年度構築した、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 から毎日午前 2 時過ぎに送られる PDF 形式の Daily Palo Alto Networks Reports (以下、日報) に基づいて調査を行うというものであった。

本年度からは、PA-5050 からの日報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ので報告する。

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 のログをみると、それぞれの「脅威/コンテンツ名」(Threat/Content Name) は「重大度」(Severity) と「リスク」(Risk) による格付がされていることがわかる。「重大度」は上位から critical, high, medium, low, informational の順であり、それぞれの「重大度」はさらに「リスク」という 5 段階の相対的評価 (1=lowest to 5=highest) がついている。

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 であってもリスク値の高い脅威については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、最上位の「重大度」 critical と判定された疑わしき脅威については、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するという設定を行った。前日のサマリーレポートである日報をトリガーとしているため、基本的に事後対応とならざるを得ないため、最上位の「重大度」については対応が後手にまわる事態を避けるための対応である。その後数ヶ月の運用を経て、業務に影響がないことを確認して上で「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　日報内容のカスタマイズ

次に行ったのは、PA-5050 からの日報内容の見直しである。運用当初はデフォルトのテンプレートによる日報送信機能を利用したため、日報は 29 ページの PDF で毎日 CSIRT メーリングリストに配信された。各ページの内容は以下の通りである。

運用当初の日報 29 ページの内容

1. スパイウェアに感染したホスト
2. 上位のアプリケーション カテゴリ
3. 上位のアプリケーション
4. 上位の攻撃者
5. 国別の上位の攻撃者
6. 上位の脅威
7. 上位の接続
8. 上位の拒否されたアプリケーション
9. 上位の拒否された宛先
10. 上位の拒否された送信元

11. 上位の宛先国
12. 上位の宛先
13. 上位の出力インターフェイス
14. 上位の宛先ゾーン
15. 上位の HTTP トンネル対象アプリケーション
16. 上位の入力インターフェイス
17. 上位の送信元ゾーン
18. 上位のセキュリティ ルール
19. 上位の送信元国
20. 上位の送信元
21. 上位のスパイウェア脅威
22. 上位のテクノロジ カテゴリ
23. 上位の被害者
24. 国別の上位の被害者
25. 上位のウイルス
26. 上位の脆弱性
27. 上位の Web サイト
28. 上位の Unknown TCP 接続
29. 上位の Unknown UDP 接続

「国別の上位の攻撃者」などは時間に余裕があるときにでも世界地理の勉強として眺めるなら良いだろうが、毎日のインデント対応業務として必須であるのは上記 29 ページ全てというわけではない。

また、たとえば「スパイウェアに感染したホスト」のページでは、PA-5050 が判断した感染ホストの上位一覧が表示されるが、本学 IP アドレス以外の学外のホストも一覧の中に表示されるため、学内ホストに限定してリストアップされるような改正が望まれていた。

さらに、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日報調査業務に参加することになったという学内事情もあり、日報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。

日報内容のカスタマイズの方針は以下の通りである。

- 本学の IP アドレス (133.60.*.*) を持つホストのみ表示する。
- 上記 IP アドレスのホストに対して、即日確認作業及びインシデント対応業務が可能な以下のリストのみ表示する。
  - スパイウェアに感染したと判断される・疑いのあるホスト
  - 上位のスパイウェア脅威を受けたと判断されるホスト
  - 上位のウイルスに感染したと判断される・疑いのあるホスト
- 実際に不審な通信が行われた脅威と通信が遮断された脅威を分けて表示する。

PA-5050 のログをみると、それぞれの脅威には「アクション」が記載されており、その種類は default, allow, alert, block, reset-server, reset-both, reset-client, drop-all-packets, drop, block-ip となっている。したがって、「アクション」が alert となっている脅威は通信が遮断されていないため、インシデント・レスポンス/レディネス対応が必要となる。

上記方針のもと、何回かの試行錯誤の後、本稿執筆時点で運用しているカスタマイズされた日報の内容は以下の通りである。

カスタマイズして運用中の日報 8 ページの内容

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）
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
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）
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
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）
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
7. 上位の攻撃者にリストアップされている学内ホスト
8. 上位の被害者にリストアップされている学内ホスト

参考までに、カスタマイズされた日報のページごとのイメージを Appendix A に示す。この日報を毎朝センター長がチェックし、1 ページ目、3 ページ目、5 ページ目に学内 IP アドレスがリストされていた場合には、当該 IP についての PA-5050 のログ収集、当該機器の利用者情報調査、そして必要があれば利用者へのウイルス対策ソフトによる完全スキャンの依頼を行うのが日課となった。また、8 ページ目の「上位の被害者」にリストアップされている学内ホストのうち、本学が契約している Office 365 以外の外部のメールサーバから pop3 等でウイルスが添付されたメールをダウンロードしたと警告がある場合は、5 ページ目のウイルスに感染したと判断されたホストと同様の対応を行うこととした。参考までに、当該機器の利用者に対して送信している調査依頼メールの例を Appendix B に示す。また当該機器の利用者情報調査に関して必要なシステムについては次で述べる。

2.3　接続情報検索システム「ヒロミル」

前節で述べたように、カスタマイズされた日報にリストアップされた、不審な通信を行っている機器については、利用者を特定し、対応を依頼することになるが、その際必要となるシステムについて述べる。

本学のキャンパス情報ネットワークへの接続方法として無線 LAN と有線 LAN による接続がある。無線 LAN サービスは Hiroin Wi-Fi と呼ばれ、センターが設置した学内 620 台余りの無線 LAN AP で構成され、全ての学生・教職員が IEEE 802.1X 認証によって利用でき、DHCP サーバによって IP アドレスが付与される。

また、有線 LAN による接続に関しては、全学的に物理アドレス認証による登録と DHCP サービスによる IP アドレスの自動付与が行われる。オプションとして、必要な場合には別途固定 IP の申請が可能であるが、多くの新規接続のパソコンについては、DHCP による IP アドレスの自動付与が標準である。

このように、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、PA-5050 の日報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有線 LAN 接続機器の物理アドレスを特定し、その物理アドレスの登録者情報を検索すること、あるいは同じく過去の特定の日時に特定の IP アドレスを付与されていた Hiroin Wi-Fi 接続者情報を検索するシステムが必要となる。

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（ひろみ））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。図 1 が「ヒロミル」の Web 画面の一部である。担当技術職員の内部利用が目的であり外部公開を想定していないため、実用本位の簡素な表示画面である。「ヒロミル」で検索・確認できる項目は多岐にわたるため、Appendix C に一覧をまとめておく。

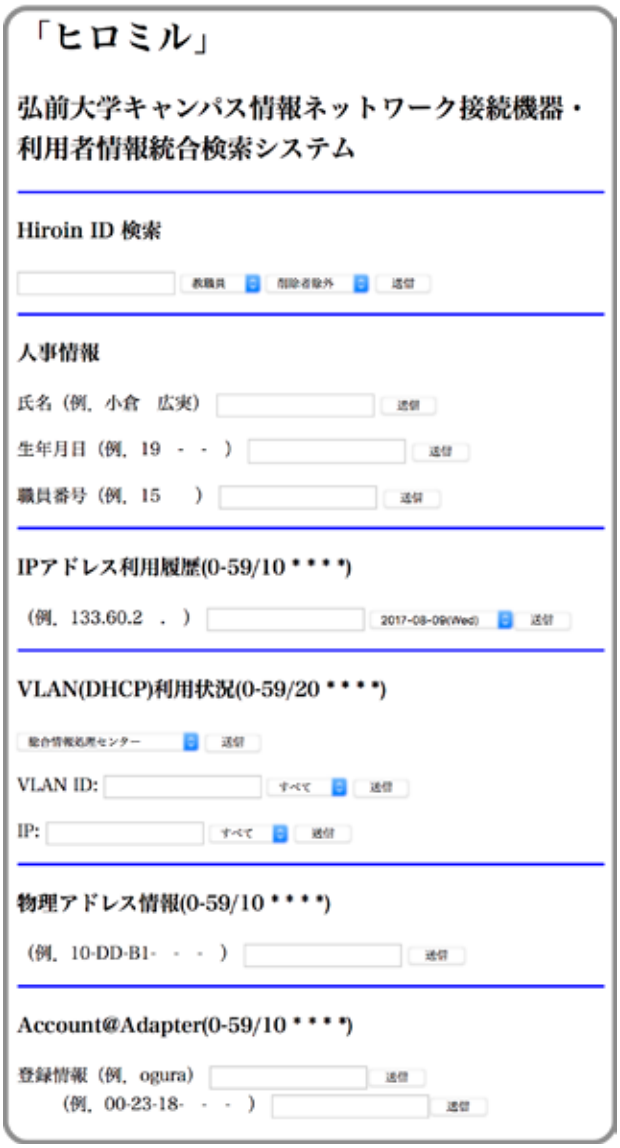
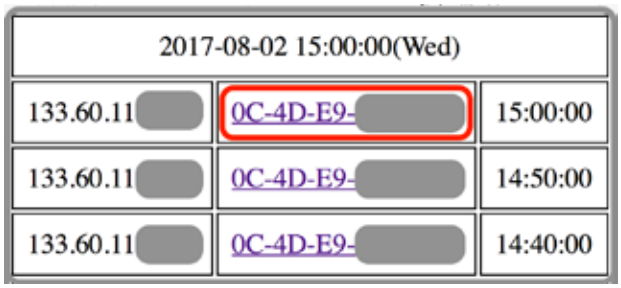


図 1. 「ヒロミル」の Web 画面の一部

「ヒロミル」には多くの検索機能があるが、日報にリストアップされた機器の IP アドレスの利用者情報を検索する例をあげると、以下のような手順になる。

まず、IP アドレス利用履歴の欄に、検索したい IP アドレス（以下の例では 133.60.11□.□□□）を入力し、前日から 1 週間前までの日付を指定して「送信」ボタンをクリックする。

図 2. IP アドレス利用履歴の検索画面

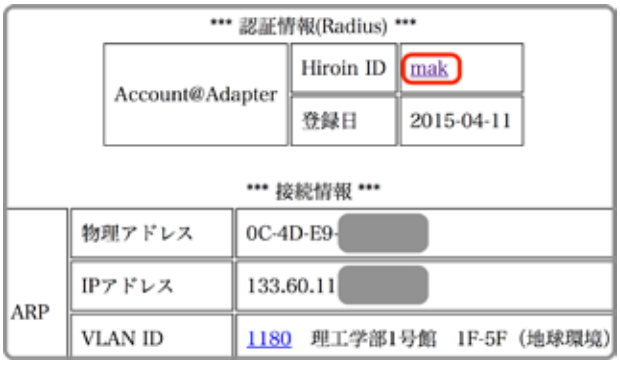


2017-08-02 15:00:00(Wed)		
133.60.11	0C-4D-E9-	15:00:00
133.60.11	0C-4D-E9-	14:50:00
133.60.11	0C-4D-E9-	14:40:00

図 3. IP アドレス利用履歴の検索結果画面

すると、図 3 のように、指定した日付の 10 分毎にその IP アドレスを使用していた機器の物理アドレスが検索結果として表示される。(図 3 の例では 0C-4D-E9-□□-□□-□□。)

この例では当該 IP アドレスは固定 IP として使用されているので、時間によらずに同一の物理アドレスが表示されているが、DHCP の場合は日時によって異なる機器の物理アドレスが表示されることになる。



*** 認証情報(Radius) ***

Account@Adapter	Hiroin ID	mak
	登録日	2015-04-11

*** 接続情報 ***

ARP	物理アドレス	0C-4D-E9-
	IPアドレス	133.60.11
	VLAN ID	1180 理工学部1号館 1F-5F（地球環境）

図 4. IP アドレス利用履歴の検索結果画面

次に、図 3. の検索結果として表示された物理アドレスをクリックすれば、その機器の登録者（利用者）の Hiroin ID と関連する登録情報が図 4 のように表示され（この例では mak)、これをもとに当該機器の登録利用者へ直接注意喚起や対応依頼を行うことが可能になる。

このように、PA-5050 の日報にリストアップされた IP アドレスをキーにして「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日報で報告された場合、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

日報 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。

4 まとめ

本稿では、弘前大学における、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）体制を整備するために行った改善点について述べた。特に強調すべきは、次世代ファイアウォール PA-5050 からのカスタマイズした日報 Daily Palo Alto Networks Reports から、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「ヒロミル」を利用して迅速な当該機器利用者情報の検索を可能にした点である。

この改善により、利用者からウイルス感染の報告が来る前に、ウイルス付きメールをダウンロードした可能性のある利用者への通知やウイルス対策ソフトによる完全スキャンの依頼が可能になった。

実際には、本学が全ての職員・学生用に契約しているメールサービス（Office 365）では、このようなウイルス付きメールがそのままの状態で配信される事例はほとんどない。しかし、本学が契約しているメールサービス以外の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 が通信遮断しているケースもあり、その場合は当該利用者に対し、学内のパソコンにダウンロードする前に、Web ブラウザでメールサービスにログインし不審なメールを削除するよう依頼することも可能である。

本学における情報セキュリティ対策の強化に際し、次世代ファイアウォールの機能を最大限に活用するために、ネットワークセキュリティ運用監視サービスの契約も一時は検討したが、費用の面でこの外注による対策は断念し、代わりに追加の費用を必要とせずに、本学技術職員がいわば手作りで対策できることは何かを考えた結果、たどり着いたのが今回報告した内容である。

今回報告した体制整備だけでセキュリティ対策は万全と言い切れるわけではないことは承知しているが、まずはこの手作りのインシデント・レスポンス/レディネス体制について、今後も必要な改善をはかりながら運用していくことで、情報セキュリティの維持・強化につなげることが我々の当面の使命であると考えている。

Appendix A

参考までに、カスタマイズされた Daily Palo Alto Networks Reports (日報) のページごとのイメージを以下に示す。表示内容の一部を省略して表示している。

1 ページ目

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)。

スパイウェアに感染したホスト

palo1_new : Monday, July 31, 2017

宛先アドレス	アクション	リスク	重大度	アプリケーション	脅威/コンテンツ名
133.60.1	alert	4	medium	web-browsing	Generic User-Agent Traffic

2 ページ目

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。

Block-IP.Drop.Reset-Both

palo1_new : Monday, July 31, 2017

[illegible]	[illegible]	アクション	リスク	重大度	アプリケーション	脅威/コンテンツ名
133.60.3	133.60.3	block-ip	4	low	sip	Sipvicious Gen User-Agent Traffic
	133.60.3	block-ip	4	low	sip	Sipvicious Gen User-Agent Traffic
	133.60.3	block-ip	4	low	sip	Sipvicious Gen User-Agent Traffic
133.60.2	133.60.2	block-ip	4	low	sip	Sipvicious Gen User-Agent Traffic
133.60.1	ach.hirosaki-u.ac.jp	block-ip	4	low	sip	Sipvicious Gen User-Agent Traffic
133.60.1	133.60.1	drop	1	critical	unknown-udp	Win32.Conficker.C p2p
133.60.1	133.60.1	drop	1	critical	unknown-udp	ZeroAccess.Gen Command and Control Traffic

3 ページ目

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)。

上位のスパイウェア脅威

palo1_new : Monday, July 31, 2017

脅威/コンテンツ名	送信元アドレス	宛先アドレス	アクション	リスク	重大度
Generic User-Agent Traffic	52.69.8	33.60.1	alert	4	medium
	202.3	133.60.1	alert	4	medium
	23.210.2	133.60.1	alert	4	medium
	23.210.2	133.60.1	alert	4	medium
Suspicious DNS Query (generic:strategy.googleapis.net)	133.60.8	133.60.1	alert	4	medium

4 ページ目

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。

Block-IP.Drop.Reset-Both .

palo1_new : Monday, July 31, 2017

脅威/コンテンツ名	送信元アドレス	宛先アドレス	アクション	リスク	重大度
Sipvicious Gen User-Agent Traffic	146.0.2	133.60.2	block-ip	4	low
	195.154.2	133.60.1	block-ip	4	low
Win32.Conficker.C p2p	93.34.14	133.60.1	drop	1	critical
	118.97.1	133.60.1	drop	1	critical
ZeroAccess.Gen Command and Control Traffic	86.240.2	133.60.1	drop	1	critical

5 ページ目

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)

上位のウイルス

palo1_new : Monday, July 31, 2017

一致データ未検出

上図のイメージのようにウイルス感染の警告がない朝は大変清々しい。

6 ページ目

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。

Block-IP.Drop.Reset-Both.

palo1_new : Monday, July 31, 2017

脅威/コンテンツ名	送信元アドレス	宛先アドレス	アクション	リスク	重大度
Virus/Win32.WGeneric.mmirf	121.29.5	133.60.1	reset-both	4	medium
Virus/Win32.WGeneric.idfly	150.138.	133.60.1	reset-both	4	medium
	222.186.	133.60.1	reset-both	4	medium
Virus/Win32.WGeneric.iwiba	150.138.	133.60.1	reset-both	4	medium
Virus/OSX.WGeneric.modyz	111.64.9	133.60.1	reset-both	4	medium

7 ページ目

上位の攻撃者にリストアップされている学内ホスト。

上位攻撃者

palo1_new : Monday, July 31, 2017

送信元アドレス	アクション	重大度	アプリケーション	脅威/コンテンツ名
133.60.2	alert	informational	web-browsing	HTTP OPTIONS Method
133.60.5	alert	informational	web-browsing	HTTP OPTIONS Method
133.60.1	alert	informational	web-browsing	HTTP OPTIONS Method
133.60.2	alert	low	web-browsing	Suspicious Abnormal HTTP Response Found
	alert	low	web-crawler	Suspicious Abnormal HTTP Response Found
133.60.1	alert	low	web-browsing	HTTP Cross Site Scripting Vulnerability
	alert	low	google-app-engine	HTTP Cross Site Scripting Vulnerability
133.60.2	alert	informational	web-browsing	HTTP OPTIONS Method
133.60.6	alert	low	web-browsing	HTTP Directory Traversal Vulnerability

8 ページ目

上位の被害者にリストアップされている学内ホスト。

上位の被害者

palo1_new : Monday, July 31, 2017

宛先アドレス	アクション	リスク	重大度	アプリケーション	脅威/コンテンツ名
133.60.1	alert	1	informational	unknown-tcp	Suspicious HTTP Response Found
133.60.1	alert	1	informational	unknown-tcp	Suspicious HTTP Response Found
	alert	4	low	web-browsing	JavaScript Obfuscation Detected
	alert	4	low	web-browsing	JavaScript Obfuscation Detected
	alert	1	informational	unknown-tcp	HTTP Non RFC-Compliant Response Found
133.60.3	alert	1	informational	unknown-tcp	Suspicious HTTP Response Found
	alert	1	informational	unknown-tcp	HTTP Non RFC-Compliant Response Found
133.60.1	alert	1	informational	unknown-tcp	Suspicious HTTP Response Found

Appendix B

カスタマイズされた日報の 1 ページ目「スパイウェアに感染したと判断された学内ホスト」の利用者に対して送信する調査依頼メールの例：

Subject: [csirt:790] **不審な通信を行っている機器の調査依頼**
From: **弘前大学** CSIRT **メンバー**
To: user-id@hirosaki-u.ac.jp
Reply-To: csirt@ml.hirosaki-u.ac.jp
CC: csirt@ml.hirosaki-u.ac.jp

＊＊部
＊＊　＊＊　様

弘前大学 CSIRT **では学内外の通信をファイアーウォールで監視しています。** 7/26(**水**) 15:44 **頃から複数回、下記の機器からスパイウェアと思われる通信が観測されました。(ファイアーウォールの通信記録を添付します。)**

検出日時：7/26 15:44 - 16:42
IP **アドレス：**133.60.1*.***
物理アドレス：6C-0B-84-**-**-**
登録アカウント：user-id
コンピュータ名：USER-PC
OS：Windows7

スパイウェアに感染している可能性がありますので、F-Secure **等のウイルス対策ソフトで「完全スキャン」していただき、結果を「弘前大学** CSIRT**」にメールでお知らせしていただくようお願いします。**
--
弘前大学 CSIRT
csirt@ml.hirosaki-u.ac.jp

Appendix C

参考までに、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「ヒロミル」で検索・確認できる項目は、本稿執筆時点で以下の通りである。

- Hiroin ID 検索 (教職員、学生、全て) (弘前大学統合認証システムのアカウントである Hiroin ID の登録情報の検索)
- 人事情報（氏名、生年月日、職員番号をキーに検索）
- IP アドレス利用履歴
- VLAN(DHCP) 利用状況
- 物理アドレス情報
- Account@Adapter 登録情報、削除情報（有線 LAN 接続の物理アドレス認証システムの要）
- FDB-Table 情報（フロアスイッチごと、VLAN ID ごとの検索）
- 固定 IP アドレス申請情報
- F-Secure 情報（キャンパスライセンスで導入しているウイルス対策ソフトの導入情報）
- VPN 利用者情報
- Eduroam 利用者情報
- FireWall 設定情報
- サーバ証明書情報
- 物理アドレス・フォーマット変換 y （大文字・小文字、ハイフン・コロン）
- メール転送設定スクリプト
- DHCP 利用状況履歴
- IP アドレス利用状況（キャンパスごとの有線 LAN 接続、Hiroin Wi-Fi による無線 LAN 接続）
- Hiroin Wi-Fi 利用状況（各部局建物ごと、2.4GHz 及び 5GHz の DHCP による IP アドレスの配布数・残数・使用率）
- 無線 LAN 認証状況 (SSID ごとの認証数、iOS, Android の接続数)
- DHCP 利用履歴（残数 10 以下の記録）
- 配布グループ（alias）（本学離職者等の転送設定の確認）
- 利用機器数（各キャンパスごと、各部局建物ごとのネットワーク接続機器数）
- 利用者不明機器リスト
- 「MAC アドレス・ベンダー検索」へのリンク
- 「ドメイン・IP アドレス検索」へのリンク
- Office 365 利用状況
  - OneDrive for Business（最大一人 1TB まで利用可）の利用上位者リスト
  - ProPlus 契約者 (一人で Windows/Mac 合わせて 5 台まで利用可）の利用状況
  - Exchange 利用状況

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.