Vol.2012-IOT-16 No.35
2012/3/16

Wiki と携帯型遠隔操作機器を使ったネットワークセキュリティ監視システム

山之上卓[†]　白澤竜馬[†]　小田謙太郎[†]　下園幸一[†]

組織のネットワーク管理者は，ネットワークのセキュリティ監視をしているとき，監視地点から見て L3 スイッチや NAT の向こう側にあるサブネットの状態を詳しく知りたいことが良くある．本発表では，Wiki を使ってこれを可能にする遠隔操作可能な携帯型ネットワークセキュリティ監視について述べる．

A Security Monitoring System consists of a Wiki Software and a Portable Remote Control Device

Takashi Yamanoue[†]　Ryoma Shirasawa[†] Kentaro Oda[†] and Koichi Shimozono[†]

A network manager of an organization sometimes wants to know the status of sub-LAN behind a L3 switch or a NAT from IDSs of the central network infrastructure. This paper discusses a network security system which consists of portable sensor devices and a Wiki software which realize to monitor the sub-LAN from the central network infrastructure.

1. はじめに

大規模な組織内 LAN では，情報セキュリティ強化のためにファイヤーウォールや IDS を設置し，組織内 LAN の情報セキュリティの状態を監視し，それによってセキュリティを強化すると共に，なにか異常を発見した場合には速やかに対応できる体制が取られている場合が多い．このような監視体制が組織の隅々で整っていれば問題は少ないが，ファイヤーウォールの設定や IDS 出力の解析を行うには，通常，それなりの経験や専門知識が必要である．このため，組織内の出入り口のところに少数のファイヤーウォールや IDS を設置し，少人数の基幹ネットワーク管理者によって監視が行われる場合が多い．近年，IDS の代わりに IPS を使う場合も増えていて管理者の負担は減少しているが，IPS では防ぎきれない侵入も依然多くある．また IPS を組織内 LAN の隅々に配置することは現状では経済的に困難であることが多い．

小さな LAN を簡単に構築し，セキュリティを強化し，ネットワークの管理運営を容易にするため NAT 機能と DHCP 機能を併せ持つブロードバンドルータが広く使われている．NAT 機能により，NAT の外部から直接この LAN 内に接続されたパソコンに接続することは困難になり，侵入が難しくなる．DHCP の機能により，この LAN 内にパソコンを接続するだけで IP アドレス等が割り当てられ，そのパソコンはネットワーク外部の Web サーバ等と通信が可能になる．大学では研究室等で独自にブロードバンドルータを用意し，それを基幹 LAN に接続して利用する場合がある．しかしながら，この LAN 内のパソコンがウィルスに感染する場合もある．

基幹ネットワーク管理者は，監視地点から見て L3 スイッチや NAT の向こう側にある LAN(これ以降，NAT-LAN)の状態を詳しく知りたいことが良くある．例えば，組織の出入り口の IDS で組織内のホストのどれかにウィルス感染の疑いが発見された場合，そのホストの通信の送信元側 IP アドレスにより，どのサブネットワークに，そのホストが接続されているかは分かるが，L3 スイッチの向こう側にそのホストがある場合，監視地点側からは具体的なホストの MAC アドレスを知ることができず，DHCP で IP アドレスが割り当てられているような場合は，簡単にホストを特定することはできない．また，ウィルスに感染したホストが NAT-LAN に接続されていることがわかった場合，当該ホストの IP アドレスすら特定することは困難になり，ホストの特定により時間がかかってしまう．

このような問題に対処するため，組織によっては，NAT の利用を禁止しているところもある．しかしながら，近年のパソコンは無線 LAN アクセスポイント付き NAT として機能する場合があり，スマートホンを Wi-Fi で利用するためにこの機能が使われる場合が多く NAT の利用を禁止してもそのことを周知徹底するのは困難になってい

[†] 鹿児島大学
Kagoshim University

る．また，NAT が禁止されると大学の研究室などでは気軽にパソコンやスマートホンなどをネットワークに接続することができなくなる場合があり，利用者の利便性を損なうことになる．

本論文では，利用者の利便性を損なうことなしに，情報セキュリティの強化を行うことを目的として開発している，ネットワークセキュリティ監視システムについて述べる．

2. システム概要

この監視システムは，ノートパソコンにネットワークインターフェースを追加した携帯型遠隔操作デバイスと，このデバイスを遠隔操作し，その操作結果を確認するための Wiki (PukiWiki) サイトで構成されている(図 1)．携帯型遠隔操作デバイスは，NAT（ブロードバンドルータ）または L3 スイッチと，NAT-LAN の LAN(Sub-LAN)の部分との間に接続する．

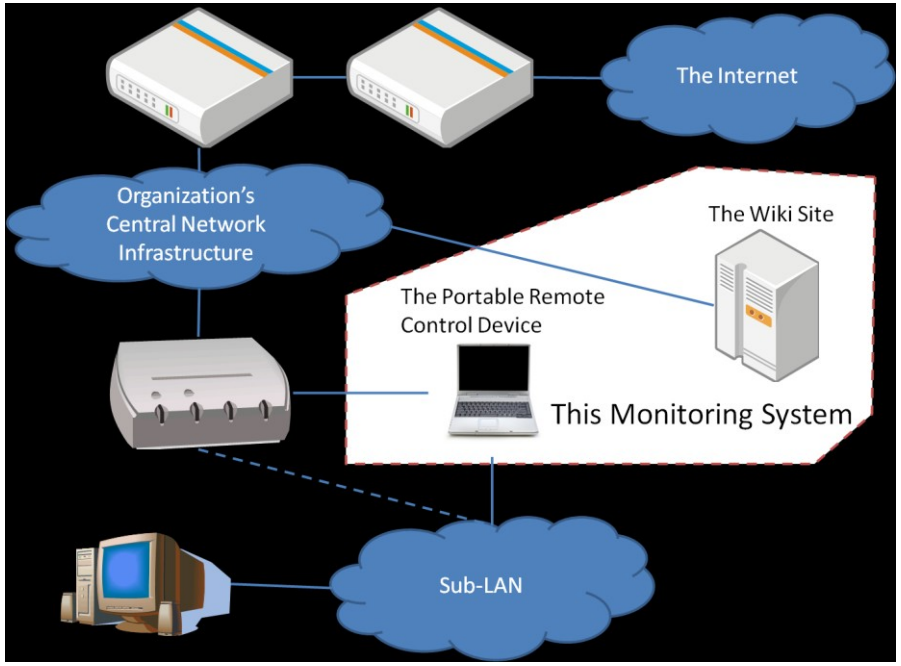

図 1　本システムの概要

ブロードバンドルータが持っている LAN ポートに直接パソコン等が接続されている場合は，スイッチを別に用意して，このスイッチとブロードバンドルータの間にこのデバイスを接続する．ブロードバンドルータが無線 LAN アクセスポイントの機能を持っている場合は，その無線 LAN アクセスポイントの機能を停止させ，別の無線 LAN アクセスポイントを Sub-LAN に接続する．Wiki サイトは，ネットワーク管理者と，この携帯型遠隔操作デバイスの双方がアクセスできる場所に接続する．

図 2 に本システムの動作の概要を示す．ネットワーク管理者は Wiki のページに携帯型遠隔操作デバイスに実行させるコマンドを記述する．デバイスの「Wiki Access Engine」は定期的にこの Wiki ページにアクセスし，コマンドを読み込み，実行し，結果をこのデバイス内の Queue に書き込むことを繰り返す．これと並行して，定期的に Queue に書き込まれた結果を読み，その結果を Wiki ページに書き込むことを繰り返す．Wiki ページに書きこまれた結果をネットワーク管理者は確認する．

本システムは，基幹ネットワークの IDS でウィルス感染を検知した後，本システムの携帯型遠隔操作デバイスを，ウィルスに感染したホストが接続されていると思われ

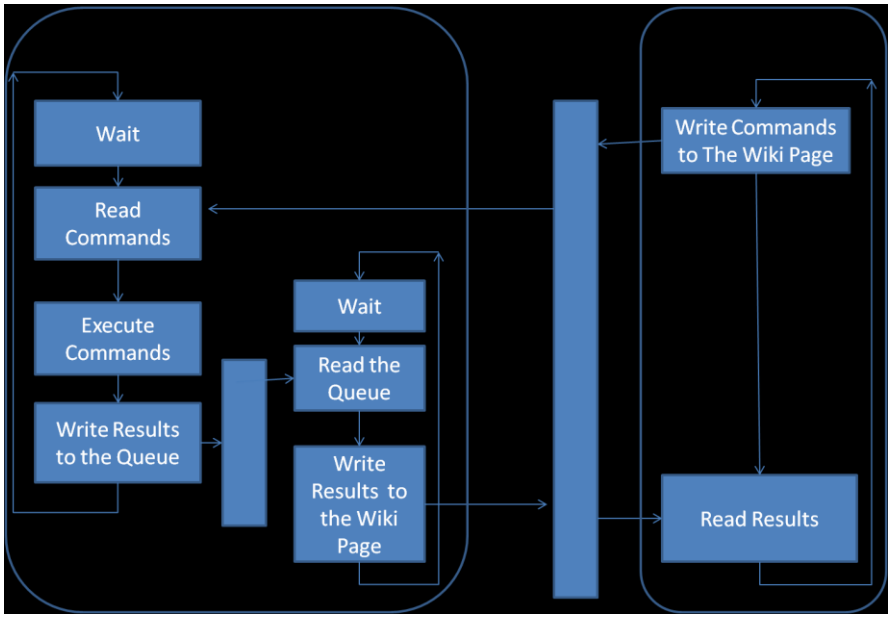

図 2. 本システムの動作の概要

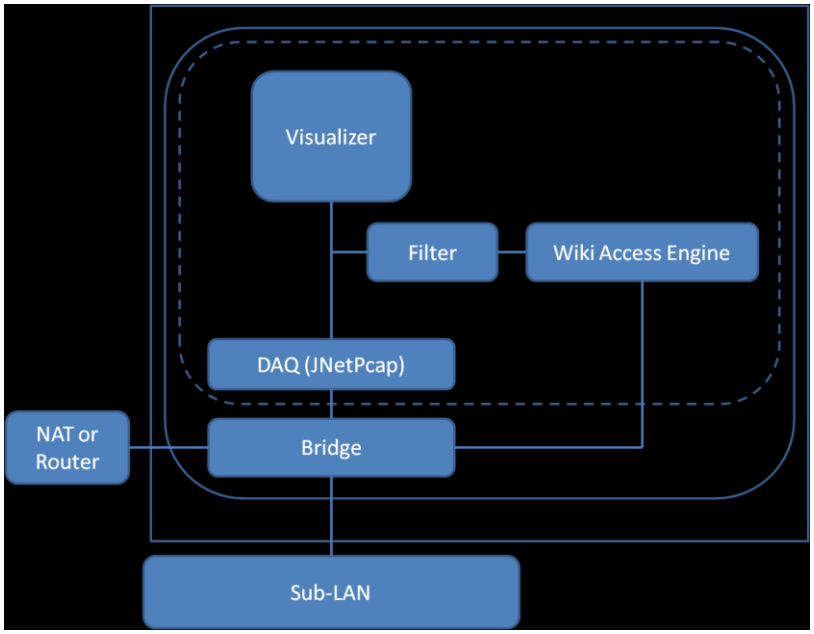

図 3　携帯型遠隔デバイス(The Portable Remote Device)の構成

る LAN に設置し, IDS で検知されたパケットがもう一度検知されたら, そのパケットを含む MAC アドレスの情報などを通知するよう, Wiki ページにコマンドを記述し, 監視を行うような運用を想定している.

図 3 に携帯型遠隔操作デバイスの構成を示す. ノートパソコン内に Linux の仮想マシンを搭載する. 仮想マシンのブリッジにより, NAT またはルータと, Sub-LAN が接続される. また, このブリッジに DAQ(Data Acquisition Library) も接続される. DAQ として, JNetPcap を利用している. DAQ で取得されたパケットは, このシステムが持つ視覚化システム(Visualizer)[7]に送られるのと同時に, Filter に記載されたパターンと合致した場合, このパケットの情報が Wiki ページに書きこまれる. Filter のパターンは, Wiki ページに書かれたコマンドが解釈実行されることにより, 記載される. Wiki Access Engine」は文献 4)5)6)のシステムを改造して作成している. 図 4 に携帯型遠隔操作デバイスの例を示す. Visualizer は文献 1)のものを元に作成している.

携帯型遠隔操作デバイスで実行されるコマンドの列は, このシステムで利用する Wiki (PukiWiki)ページ上の Pre-format された部分の中で,

図 4. 携帯型遠隔デバイスの例

command: <コマンド>

の繰り返しにより記載される. コマンドの実行結果は, コマンドの列の後に記載された,

result

の後に書きこまれる.

3. 利用例

3.1 起動と初期設定

携帯型遠隔操作デバイスのノートパソコンを NAT またはルータと Sub-LAN の間に接続した後, Linux の仮想マシンを起動し, 仮想マシンの中で管理者権限でコマンド

trafficviewer

を実行する. これにより, 図 5 のような注意を促すウィンドウが表示される.

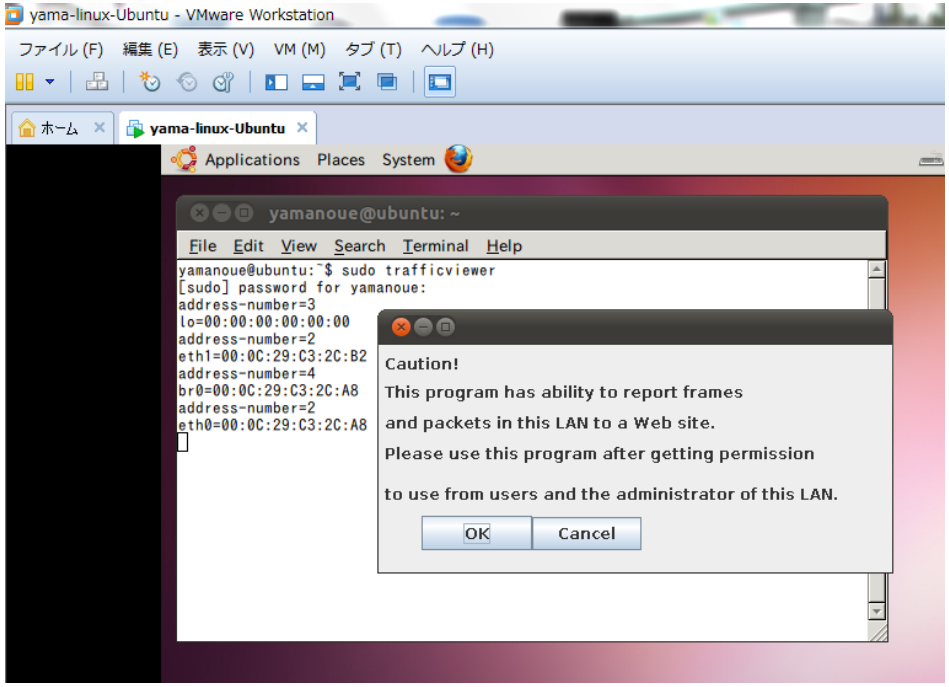

図 5. 起動と起動後の最初の注意を促すウィンドウ

このウィンドウで「OK」ボタンをクリックすると，図 6 のような LAN 内通信視覚化表示ウィンドウが表示される．初期設定を行う場合は，ここで，「Setting」ボタンをクリックする．「Setting」ボタンをクリックすると，図 7 のような設定ウィンドウが表示される．このウィンドウで「main-tab」を選択すると，監視インターフェースの設定画面が表示される．この画面では Linux 仮想マシンで利用できるネットワークインターフェースの一覧表が表示されている．監視するインターフェース（br0）をクリックするとインターフェース br0 が選択され，その行の「cap」の欄に「!」が表示される．「PukiwikiCommunicator」タブを選択すると，図 8 の設定画面が表示される．
「manager url:」の右の欄にこの画面で使用する Wiki ページの URL を設定し，このページに記載されるコマンドを読みに行く時間間隔，コマンドの実行結果を Wiki ページに書きこむ時間間隔などを設定する．「save setting」ボタンをクリックすると，設定した値が保存される．「hide」ボタンをクリックすると設定ウィンドウが閉じられる．

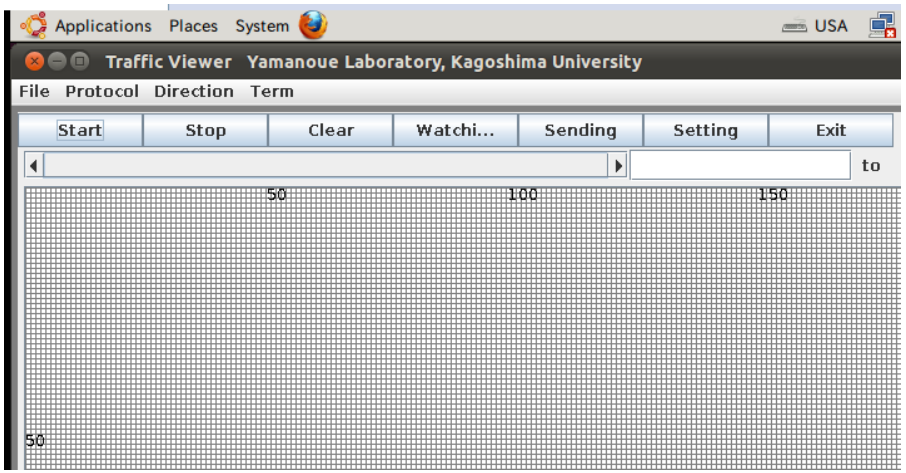

図 6. LAN 内通信視覚化表示ウィンドウ

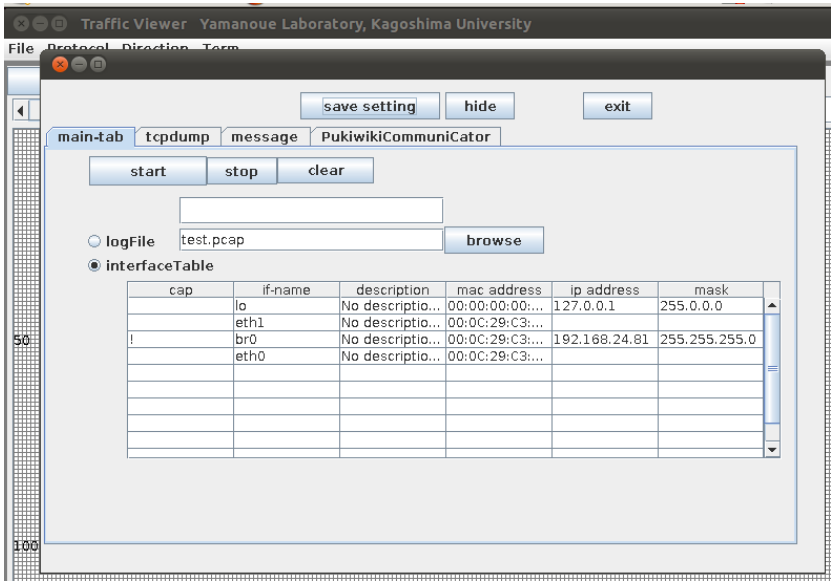

図 7. 設定ウィンドウ – 監視インターフェース設定画面

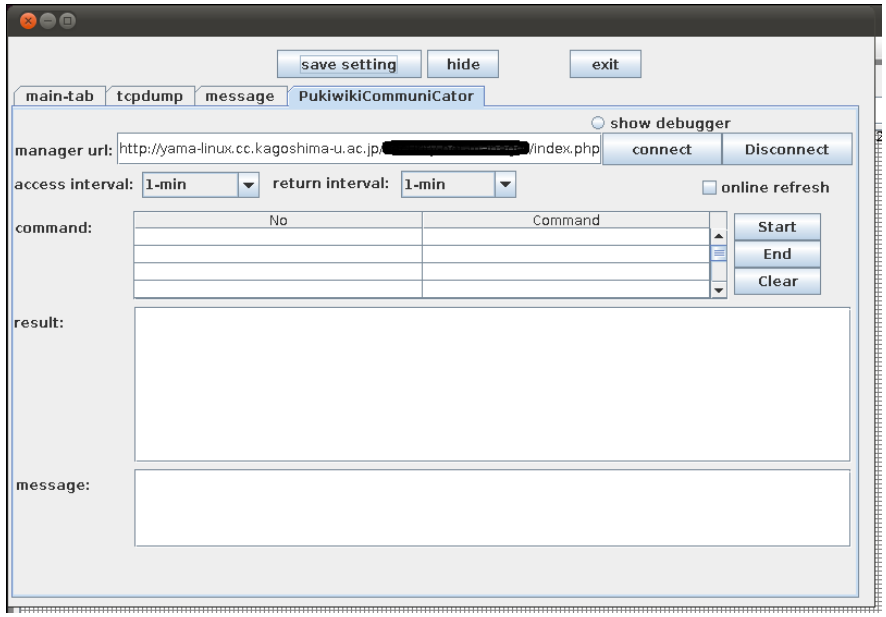

図 8. Wiki アクセスに関する設定を行う画面

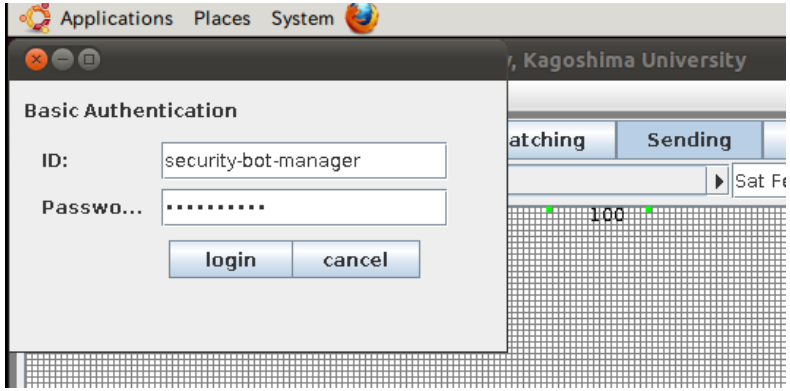

図 9. 認証画面

3.2 監視の開始

図 6 の「Start」ボタンをクリックすると，DAQ からのパケットの取得が開始される．「Sending」ボタンをクリックすると，Wiki ページへのアクセスの実行が開始される．Wiki ページのアクセスに認証が必要な場合，図 9 のような認証画面が表示される．ここで ID とパスワードを入力し，「login」ボタンをクリックする．図 6 の「Watching」ボタンをクリックすると定期的な Wiki ページに書かれたコマンドの実行と結果の書き込みが開始される．監視が開始され，Wiki ページへのアクセスとコマンドの読み込み，書き込みが正常に実行された場合，設定ウィンドウの Wiki アクセスに関する設定画面に読み込まれたコマンドや，パターン照合に成功したパケットの情報が図 10 のように表示される．

図 11 に Wiki ページに記載されたコマンド列とその実行結果の例を示す．ここで，コマンド

get ip=<IP アドレス>

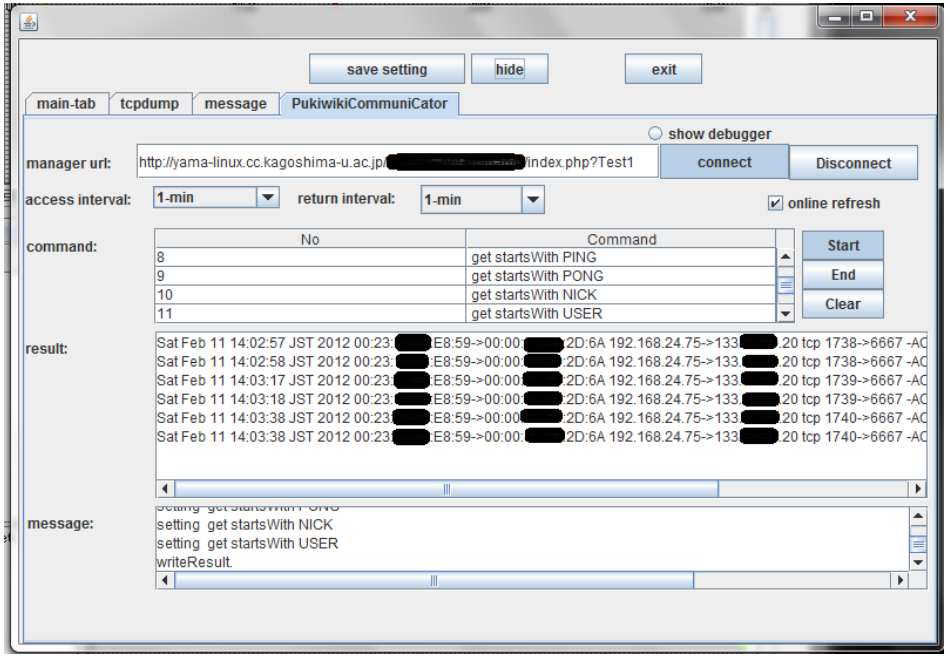

図 10. Wiki ページへのアクセス，コマンドの実行，実行結果の書き込みが行われた時の Wiki アクセスに関する設定画面

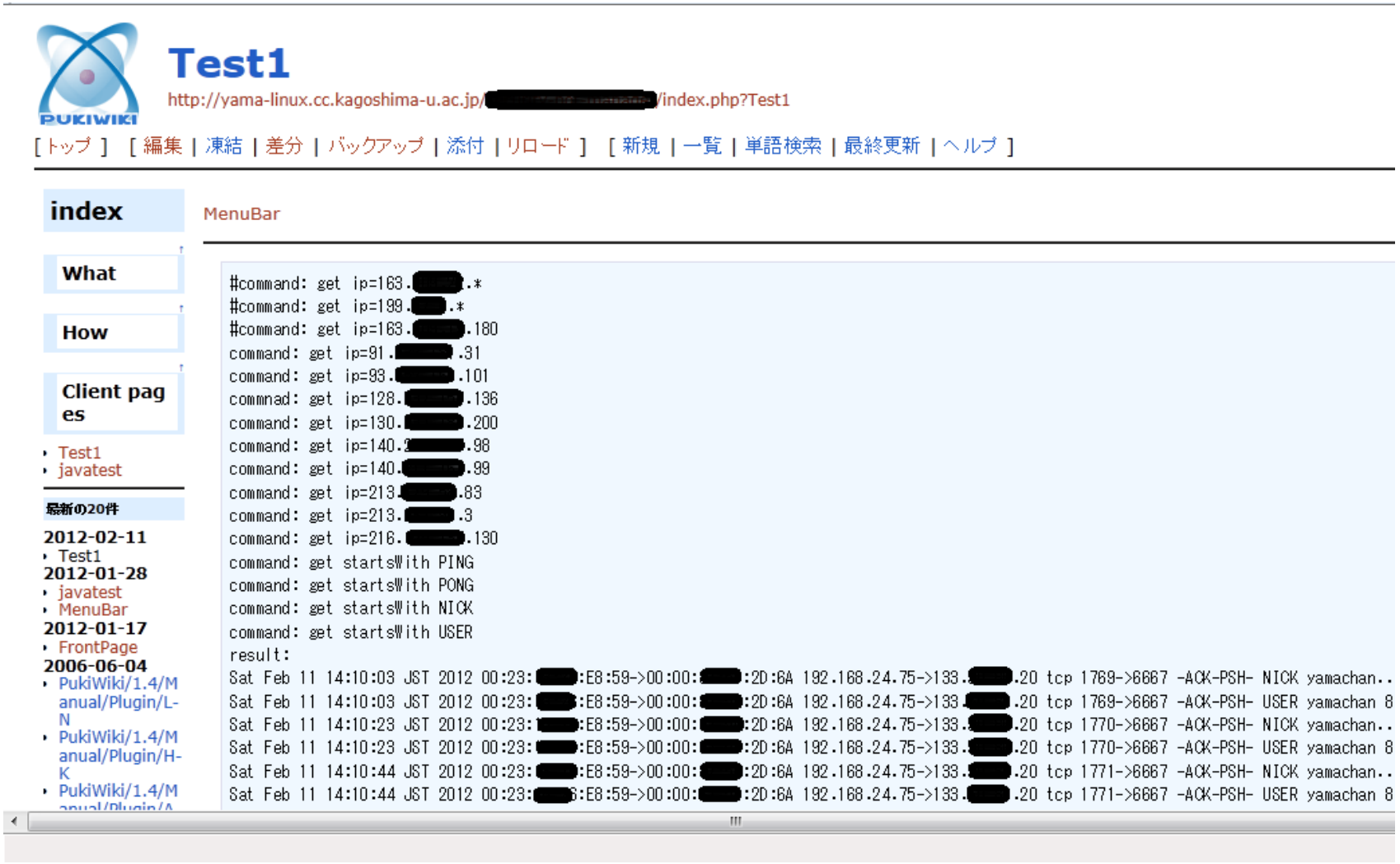

図 11. Wiki ページに記載されたコマンドの列とその実行結果の例

はDAQで入力したパケットの送信元または宛先IPアドレスが<IPアドレス>と一致した場合，その情報をWikiページに書き込むことを表す．

get startsWith <文字列>

はペイロードの先頭と<文字列>が一致した場合，その情報をWikiページに書き込むことを表す．この例の場合，PING, PONG, NICK, USERはIRCで使われるコマンドの一部である．左端が#で始まっている行はコメントである．

result: の行の下から，コマンドの実行結果が表示されている．各行はコマンドで指定されたパターンと一致したパケットの，その入力時刻，そのパケットを含むフレームの送信元と宛先MACアドレス，IPパケットの送信元と宛先IPアドレス，プロトコル，送信元と宛先ポート番号，ペイロードの先頭部分が表示されている．この例では，監視しているSub-LANのホストがIRC通信を行った時の情報が表示されている．MACアドレスを知ることができるため，この通信を行ったホストの特定が容易になる．

4. 関連研究

オープンソースのIDSとしてSnort[9]が良く使われている．Snortはシグネチャの自動更新機能も持つ．ACIDにより，Webでネットワークの状況を確認することもできる．しかしながら，NATの背後のSub-LANにSnortを設置し，監視する場合，外部からSnortの設定変更を行ったり，監視結果を外部で確認したりすることは困難である．

山井らはNATの背後にあるMACアドレスを，外部から識別する方法を述べている[2]．しかしながら，この方法は既存のNATルータをここで提案されている新たなNATルータで置き換える必要が生じる．

石田らはSNMPに対応していないネットワーク対応機器を別のシステムで補う方法を提案している[3]．このシステムは，対象のネットワーク対応機器の通常の通信はそのまま通過させ，管理に必要な通信のみ代理応答させる機能を持っており，本システムと類似している．しかしながら，NATの外部との相互通信機能は持っていない．

Kaseyaのパソコン管理システム[8]やFuruno SystemsのLANアクセスポイント管理システム(UNIFAS)[10]は本システムと同様に，定期的にエージェントプログラムがWebサーバにアクセスし，そこに書かれた指示をエージェントが実行し，結果をWebサーバ側に戻すことを行っている．エージェントプログラムとWebサーバはNATを超えて相互に通信できる．しかしながら，これらのシステムはセキュリティ強化を目的としたものではない．また，これらのシステムに特化したWebサーバを必要とする．

5. おわりに

NATやルータの背後にあるLANの状況を，遠隔操作可能な携帯型デバイスとWikiを使って監視するシステムについて述べた．遠隔操作を行う側には特殊なサーバを必要とせず，汎用的なWikiが使われる．今後，利用できるコマンドを増やしたり，Snortと連携させたりして機能を強化していく予定である．

参考文献

1) 新川拓也，山之上 卓: IPアドレスとポートによる二次元平面を用いた通信トラフィックの可視化について，情報処理学会研究報告 2006-DSM-043,pp.31-36(2006)
2) 山井成良，村上亮，岡山聖彦，中村素典:内部ネットワーク上のホストを外部から 識別するための MACアドレス中継型 NATルータ，情報処理学会論文誌, Vol.52, No.3, pp. 1348-1356(2011)
3) 石田正人，中野宣昭，桝田秀夫: ネットワーク機能をついかできる透過型代理通信システムの実装とその評価，インターネットと運用技術シンポジウム 2011, pp.9-15(2011).
4) Takashi Yamanoue, "A Draw Plug-in for a Wiki Software", saint, 10th IEEE/IPSJ International Symposium on Applications and the Internet, pp.229-232, 2010.
5) Takashi Yamanoue, Kentaro Oda, Koichi Shimozono: PukiWiki-Java Connector, a Simple API for Saving Data of Java Programs on a Wiki, ACM WikiSym '11, Proceedings of the 2011 international symposium on Wikis, Mountain View, CA, USA, 3-5 oct.,(2011)
6) Takashi Yamanoue, Kentaro Oda, Koichi Shimozono: A Simple Application Program Interface for Saving Java Program Data on a Wiki , Advances in Software Engineering, Hindawi Publishing Corporation, 2012 (in Press).
7) 山之上卓，小田謙太郎，下園幸一: 過去の状況の変化をさかのぼって表示できるLAN内通信可視化システム，情報処理学会研究会報告 2012-IOT-16 (2012)(予定)
8) KASEYA: http://www.kaseya.com/
9) SNORT: http://www.snort.org/
10) UNIFAS: http://www.furunosystems.co.jp/product/unifas.html#unifas01