Vol.2014-CSEC-66 No.51
Vol.2014-SPT-10 No.51
2014/7/4

マルチレイヤ・バインディング・ルータによるサイバー攻撃対策の提案と，OpenFlow を用いた実装評価

小林浩† 八槇博史† 末廣友貴† 上野洋一郎† 佐野香† 佐々木良一†

アドレス詐称パケットやサイバー攻撃パケットのインターネットへの流出／流入阻止を目的としたマルチレイヤ・バインディング・ルータ（MLBR）を提案する．これは，(1) ノードもしくはエンティティから接続要求があった時，その真正性を認証し，認証レベルに応じて提供する通信サービス品質（QoS）を決定する，(2) 接続要求のあったポートまたはチャネルをキーに，ノードもしくはエンティティの IP アドレスと MAC アドレスとの対をバインディングテーブルに登録する，(3) パケットを受信したポートまたはチャネルをキーにバインディングテーブルを検索し，受信パケットの送信元 IP アドレスと送信元 MAC アドレスの対が存在するときは，次ホップノードへ指定された QoS で転送し，存在しないときはアドレス詐称パケットと見なして廃棄する，(4) 他のノードからの廃棄要請を受けて，以後，該当する攻撃パケットを廃棄する，さらに，(5) インターネット利用者側に egress MLBR を，インターネット側に ingress MLBR を配備することによって，攻撃パケットのインターネットへの流出／流入を阻止することを骨子とする．

OpenFlow を用いた小規模なテストベッドを構築し，テレビなどの IEEE802.1X 非対応ノードに対する ARP リフレクションによる認証処理実験，SYN Flood 攻撃ツールを用いたアドレス詐称パケットの遮断実験，OpenFlow スイッチの性能評価などを行い，所望の機能・性能を発揮することを確認した．

A Proposal of Multi-Layer-Binding Router to Prevent Cyber-Attacks, and its Implementation and Evaluation using OpenFlow

HIROSHI KOBAYASHI† HIROFUMI YAMAKI† YUKI SUEHIRO†
YOICHIRO UENO† KAORU SANO† RYOICHI SASAKI†

An architecture of a multi-layer-binding router (MLBR) that aims for preventing outflow and inflow of IP spoofing packets or cyber-attack packets to the Internet is proposed. It consists of the following functions; (1) When a node or entity requests connection, an MLBR judges its authenticity and authenticates it, and then decides the quality of service (QoS) to be offered according to the authenticity level. (2) the MLBR registers the pair of the IP and the MAC addresses of the node or entity into a binding table, using the connection requested port or channel as the key of the entry. (3) When the MLBR receives a packet, it searches the binding table using the port or channel that received the packet as the key. If the pair of source the IP and the MAC addresses exists on the table, the MLBR forwards the packet to the next-hop node at the assigned QoS. If not, the MLBR discards the packet regarding it as a spoofed IP packet. (4) After receiving destruction requests from other nodes, the MLBR discards the corresponding attack packets. (5) Cyber-attack packet outflow and inflow to the Internet are prevented by deploying an egress MLBR to user side and an ingress MLBR to the Internet side.

A small-size test-bed using OpenFlow was constructed. Certification processing experiment by ARP reflection for IEEE802.1X non-compliant node such as TV, interception experiment of IP spoofing packets using SYN-flood attack tool, and performance evaluation of OpenFlow switch were performed. As a result, it was confirmed that it exerts the expected function and performance.

1. まえがき

年々巧妙化・組織化しているサイバー攻撃は，2011 年全世界で 0.3〜1 兆米ドルの損害を与えたと言われるほど，地球規模での大きな脅威となっている[1]．とりわけ，ボットウィルスに感染した無数の PC でボットネットを形成し，それを操り Web サイトなどへ攻撃を仕掛ける DDoS 攻撃は，これまでの「自分を守ろうとするセキュリティ技術」では防ぐことができず，「インターネット全体での取り組み」が必要となっている．

ところで，警察庁の発表によれば，2012 年中に観測されたボットネットによる攻撃では，約 97%が SYN flood 攻撃と UDP flood 攻撃で，その大半が送信元 IP アドレスを詐称していたことが特徴となっている[2]. IP アドレス詐称対策を行うことが，サイバー攻撃対策として大きな効果を挙げるものと期待される．

本稿では，ポートまたはチャネルと，送信元 MAC アドレス及び送信元 IP アドレスとの対応関係を管理し，この対応関係から外れたパケットをアドレス詐称パケットとみなして廃棄する，さらに，これをすり抜けてインターネットに流入した攻撃パケットを検出したノードからの廃棄要請を受けて，以後，該当するパケットを廃棄するマルチレイヤ・バインディング・ルータ（以下，MLB ルータもしくは MLBR と呼ぶ）を，利用者側とインターネット側とに配備することによって，攻撃パケットのインターネットへの流出／流入を阻止するサイバー攻撃対策を提案する．

以下に，アドレス詐称ひいてはサイバー攻撃対策を行う上での課題を整理した後，MLB ルータについて詳しく論じ，

† 東京電機大学
Tokyo Denki University.

さらに OpenFlow による実装とそれを用いた評価実験について述べる．

2. サイバー攻撃対策における課題

2.1 これまでのアドレス詐称対策

IP アドレス詐称が成功する背景には，インターネット上でのルーティングがパケットの宛先 IP アドレスだけを見ていることにある．IP アドレス詐称パケットのインターネットへの流入を阻止しようとするイングレス・フィルタリング技術の一つに uRPF（Unicast Reverse Path Forwarding）があるが，ネットワークアドレスのアドレス空間内のパケットを中継転送としてしまう不完全性のため，広く導入するまでには至っていない[3].

また，予め決められた端末以外がネットワークにアクセスしないように，認証によってポートに疎通許可を与える IEEE802.1X 規格がある．これに MAC アドレスベースのフィルタング機能を付加して，たとえリピータハブを介して未認証端末からフレームが送信されても阻止できる製品もあるが，データリンク層での対策であるため，認証を受けた端末がボットウィルスなどに感染し IP アドレス詐称パケットを送信しても，認証 LAN スイッチはそれを阻止することはできない[4].

さらに，企業などの内部ネットワーク向けに，DHCP によるアドレス割り当てを監視し，それと整合しないパケットをフィルタリングする DHCP snooping 技術や，単一のポリシーのもとに情報へのアクセス認可などをコントロールする Trusted Network Connect 技術，他にも IP アドレス詐称パケットの発信源を特定しようとする IP トレースバック技術など，様々な試みや製品が出回っているが，いずれもサイバー攻撃を根絶する有効な解決手段とはなっていない.

2.2 インターネット文化とサイバー攻撃対策

次に，インターネット文化とサイバー攻撃対策との関わりについて論じる．インターネットは，様々なポリシーのもとにインターネット・サービス・プロバイダー（以下，ISP）が自律的に運用しているネットワークを相互接続したものである．サイバー攻撃はインターネット全体の問題であり，IP アドレス詐称対策を部分的に導入してもその効果は微々たるものである. 無数に存在する ISP や様々な組織，一般利用者のほぼすべてに対策の導入を求めることは極めて困難なことのように思えよう．

ところで，インターネット文化には，TCP／IP や DNS，メールなどのインターネット基盤技術の開発の原動力となった「情報は共有されるべき」や，民主主義の根幹をなす「情報は広く公開されるべき」，政府や官僚，大企業の介入を嫌う「権力は横暴で信用できない」，とともに「クラッキング行為は戒めよ」がある．

すなわち，民主主義に根ざしたインターネットは，利用者の良識ある行為・行動を前提としており，利用を監視したり制限したりするメカニズムや組織はない．あるのはプロトコルの標準化を行う IETF や，ドメイン名や IP アドレスなどの有限なインターネット資源を管理する ICANN などのインターネットガバナンスだけである．インターネットはオープンだが無防備であり，これを悪用したクラッキング行為は厳に戒めるべきとする考えが，インターネットの根底にある[5].

アドレス詐称パケットは，本人が認識しているか否かはともかく，何等かのクラッキング行為を意図したパケットであることは明らかである．すなわち，アドレス詐称パケットがインターネットに流入しないような対策を講じることは，インターネット文化の考え方に沿うものと言えよう．

そして，インターネットの世界は契約で成り立っており，限られた数の一次 ISP の下に，二次／三次 ISP さらに利用者が契約し接続している．従って，一次 ISP が本提案の費用対効果を認識し導入を決断すれば，下位の ISP／組織ユーザ／一般利用者を含めた契約条項として導入を規定することができる．

しかしながら，多様なポリシーのもとで運用している ISP や様々な組織，一般利用者の行為・行動を監視・制御したり，ポリシーの強制もしくは IP トレースバックに見られるように ISP のポリシーを抉り出したりするような対策は，受け入れられ難い．すなわち，発信元 IP アドレスを詐称しているか否かなどを利用者側の出口とインターネット側の入り口とでチェックし，アドレス詐称パケットや攻撃パケットであれば，それらを確実に遮断できる必要最小限にして汎用性・実効性，そして技術的に実現可能な永続性のある対策であることが課題と言える．

これは，仮に「なんでも繋がせる」ポリシーの ISP のネットワークや匿名ネットワークがあったとしても，その存在を否定するものではなく，これらのネットワークとの接続点での検疫を強化し，さらにインターネットに向かう方向の帯域を狭めることによって，攻撃パケットのインターネットへの流入を抑制すれば良いことを意味する．すなわち，上述の課題を満たし得る対策であれば，国際法の制定などを待たずに，民間ベースの契約で地球規模での導入が可能と考えられる．

2.3 サイバー攻撃対策の対象とすべきノード

図 1 に示すように，サイバー攻撃対策の対象となるノード（ホストとルータを総称する用語としてノードを用い，さらにインターネットの階層的かつ回帰的な構造からノードの集合であるネットワークもノードとして扱う）は，多岐にわたる. IEEE802.1X などによりその真正性の認証が可能なパソコンやサーバはもとより，「何でも繋がせる」ネットワークや匿名ネットワーク，最近では家庭用ルータやテレビなどのスマート家電に遠隔操作で不正プログラムが埋め込まれ，サイバー攻撃に加担させられたとの報告もある[6]．OS やアプリケーションプログラムなどのバージョン

Vol.2014-CSEC-66 No.51
Vol.2014-SPT-10 No.51
2014/7/4

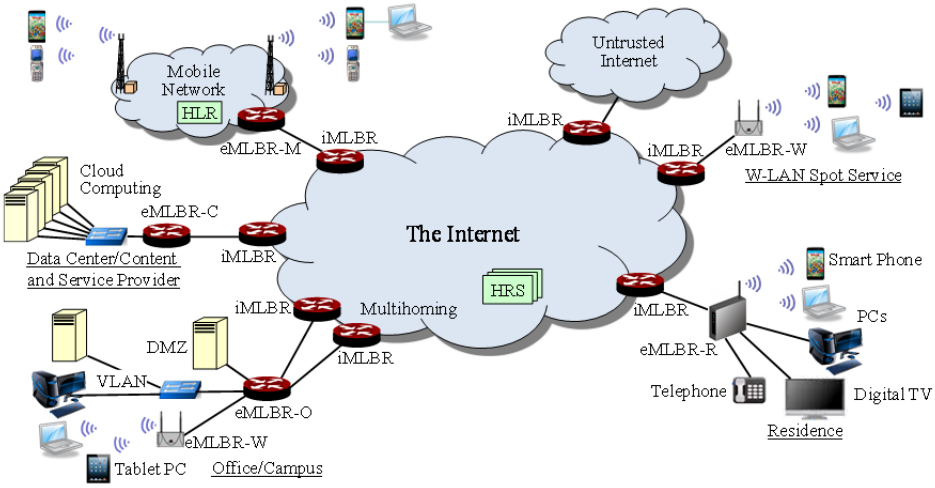


図 1　iMLBR と eMLBR とによるサイバー攻撃対策のイメージ
Figure 1　An image of cyber-attack measures incorporating iMLBR and eMLBR

アップができない無防備な，そして無数に存在する既設のノードも対策の対象としなければならない．

3. MLB ルータによるサイバー攻撃対策の提案

3.1 MLB ルータの概要

提案する MLB ルータは，

(1)　ノードもしくはエンティティ（利用者やプロセスなど）からの接続要求があった時，その真正性を判定し認証するとともに，認証レベルに応じて提供する通信サービス品質（QoS）を決定する，

(2)　接続ポートまたはチャネルをキーに，ノードもしくはエンティティの IP アドレスと MAC アドレス，QoS などとの対応関係を記憶しておくバインディングテーブル（以下，BIND テーブル）に登録する，

(3)　パケットを受信したポートまたはチャネルをキーに BIND テーブルを検索し，このパケットの送信元 IP アドレスと送信元 MAC アドレスなどの対が存在するときは，次ホップノードへ指定された QoS で転送し，存在しないときはアドレス詐称パケットと見なして廃棄する，

(4)　ポートまたはチャネルを介して適宜ノードもしくはエンティティの実在確認を行い, BIND テーブルを更新（有効期間を延長）する，

(5)　他のノードからの廃棄要請を受けて廃棄テーブルを更新し，以後，廃棄テーブルに該当するパケットを廃棄する，

(6)　インターネット利用者側に配置する eMLBR（egress MLBR）によりインターネットへの攻撃パケットの流出を，インターネット端部に（エッジルータとして）配備する iMLBR（ingress MLBR）により eMLBR をすり抜けた攻撃パケットのインターネットへの流入を阻止する，

ことを骨子とする．

(1) 項の認証は，パソコンなどの IEEE802.1X 対応ノードと，テレビなどの非対応ノードとに分けられる．IEEE802.1X には，MD5 や PEAP などいくつかの認証方法が規定されているが，後述の具体化例で用いる TLS は，MACsec によるセキュアチャネルを形成するもので，高いセキュリティレベルが得られる．非対応ノードについては，後述の ARP リフレクションによって，IP アドレスと MAC アドレスの真正性を検証し認証するが，認証レベルは低いため，QoS を例えば上り帯域を 10kbps にするなど，利用者が違和感を持たない範囲で帯域制限する方法が考えられる．なお，QoS としては MACsec による秘匿通信，前述の帯域制限や検疫，通信先が限定される M2M（Machine to Machine）型ノードに対する接続先アドレス制限などが考えられる．

(2) 項の BIND テーブルには，接続対象がサーバであれば，(well-known) ポート番号も加えることによって，不正侵入用のポートが作られても同ポートからの情報流失などを防ぐことが可能になる．

(4) 項の実在確認は，MACsec を用いるケースでは共有鍵の更新によって，またノードが別のポートもしくはチャネルに移動したときは，元のポートもしくはチャネルでの不在を確認してから，新たに認証し直し BIND テーブルのポートもしくはチャネルのみ変更すればよい．

以上の対策によって，アドレス詐称パケットのインターネットへの流出／流入，ひいてはサイバー攻撃が激減するものと考えられるが，アドレス詐称を伴わない攻撃（例えば，遠隔操作によってアドレス詐称せずに攻撃に加担させられるケースや，匿名ネットワークを経由してきた攻撃）は，防ぐことができない．(5) 項は，不正アクセス監視システム／侵入検知システム IDS やウィルス検知ソフトなどを稼働させたノードから送られてくる被害情報を分析・集約し，サイバー攻撃の判定を担う機関などのノードが発信する廃棄要請を，eMLBR 及び iMLBR が個別（攻撃パケットの送信元 IP アドレスが限定さる場合）あるいは一斉（大

規模な攻撃の場合）に受け，以後の攻撃パケットのインターネットへの流出／流入を阻止する．

ただし，（5）項は匿名ネットワークに対する対策としても有効に機能すると思われるが，これは自分たちに都合が悪い情報の発信やサービスなどの規制，すなわち前述の「権力は横暴で信用できない」に繋がりかねない側面を持つ．民主的な運用組織やルール作りが課題であり，慎重な議論が求められる．

図 1 は，以上の対策をインターネット全体に適用したイメージを表したものである．インターネットには HRS（Home RADIUS Server），移動体通信網には HLR（Home Location Register）を配し，クライアントの認証に当たる．インターネットの端部に配置される iMLBR は，基本的には同じ機能を有する．一方，利用者側に配置される eMLBR は，家庭用の-R，企業などの組織用の-O，無線 LAN スポットサービス用の-W，データセンター用の-C など，用途・形態に応じて実装される機能（無線通信，DHCP，NAPT，VLAN など）の組合せは異なるが，上述の（1）～（5）項の機能は，iMLBR と eMLBR に共通であり，（6）項により攻撃パケットのインターネットへの流出／流入を阻止する．

3.2 具体化例

(A) IEEE802.1X 対応端末

図 2 は，IEEE802.1X 対応ノードもしくはエンティティと eMLBR 間での認証及び上りパケットの転送シーケンスの例を示したものである．

クライアントのサプリカントが，拡張認証プロトコル EAPOL により，EAP メッセージフレームを eMLBR 制御部のオーセンティケータに送る．EAPOL を受け取った eMLBR は EAP 要求（TLS）を返送し，ノード及び eMLBR 間で EAP メッセージ交換を行い，eMLBR はこれを HRS へ仲介する．認証結果を HRS が eMLBR へ返すと，eMLBR のオーセンティケータは認証結果を判別し，認証に失敗したときはノードに EAP 失敗を告げ処理を終了する．認証に成功したときはノードに EAP 成功を伝えるとともに，ノードと eMLBR との間で共有鍵の生成・交換を行い，セキュアチャネルを確立する（S111～S119）．

認証に成功したノードが DHCP 要求をブロードキャスト送信すると，eMLBR は認証レベルをもとに QoS と有効期間（例えば 4 時間）を設定するとともに，セキュアチャネルの識別情報をキーに，ノードの MAC アドレスと，ノードに固定的あるいは動的に割当てる（プライベート）IP アドレス，QoS との対応関係を制御部の BIND テーブル A に仮登録のうえ，転送部の BIND テーブル A に正登録する．そして，ノードへの DHCP 応答として，名前解決サーバやデフォルトゲートウェイ（DGW）の IP アドレスなど，ネットワークへの接続に必要な情報とともに，割当てた IP アドレスを回答する（S120～S123）．

以後，ノードは eMLBR との間に確立したセキュアチャネルを介して，すなわちユーザパケットを共有鍵で暗号化し MAC フレームにカプセル化して送信し，eMLBR は暗号化ユーザ MAC フレームをデカプセル化／復号化／メッセージ認証を行った後，セキュアチャネルの識別情報をキー

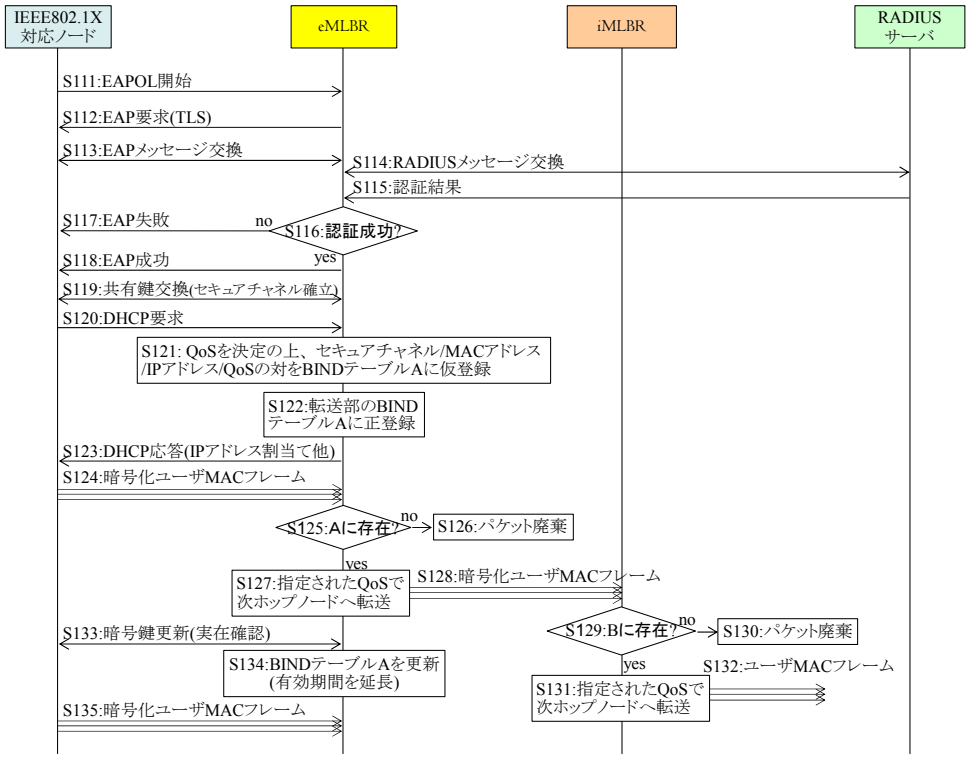


図 2　IEEE802.1X 対応ノードの認証及びパケット転送シーケンスの例
Figure 2　An example of certification for IEEE802.1X compliant node and sequence of packet forwarding

Vol.2014-CSEC-66 No.51
Vol.2014-SPT-10 No.51
2014/7/4

に転送部の BIND テーブル A を検索し，送信元 IP アドレスと MAC アドレスの対が存在しないときは，同パケットを破棄する（S124～S126）．

一方，BIND テーブル A に存在するときは，指定された QoS で，またプライベート IP アドレスを割り当てた場合には eMLBR のグローバル IP アドレスに変換（NAPT）してから，eMLBR と iMLBR との間ですでに確立しているセキュアチャネルを介して，ユーザパケットを次ホップノードである iMLBR に転送する．iMLBR は受信した暗号化 MAC フレームをデカプセル化／復号化／メッセージ認証してから，eMLBR との間のセキュアチャネル識別情報をキーに BIND テーブル B を検索し，送信元 IP アドレスと送信元 MAC アドレスの対が存在しないときはパケットを廃棄し，存在するときは指定された QoS にて次ホップノードにユーザ MAC フレームを転送する（S127～S132）．

また，eMLBR はノードもしくはエンティティとの間で共有鍵の更新による実在確認を適宜行い，確認結果に応じて BIND テーブル A を更新，すなわち有効期間を延長する（S133～S134）．

なお，ノードまたはエンティティの認証や実在確認の際に，OS やファイアウォール，ウィルス検知ソフトウェアなどの設定・更新状態を調べ，さらにそれまでの MLBR によるパケット廃棄履歴を QoS の決定に反映させることによって，利用者に対して端末をよりセキュアな状態に保つよう促すことも可能と思われる．

(B) ARP リフレクション

図 3 は，IEEE802.1X 非対応ノードの ARP リフレクション（以下，ARPF）を用いた認証及び上りパケットの転送シーケンスの例を示したものである．

ネットワークに接続したノードは，DHCP 要求をブロードキャスト送信する．DHCP サーバを兼ねた eMLBR は，要求フレーム／パケットを受信したポートをキーに，ノードの MAC アドレスと，割り当てる（プライベート）IP アドレスの対応関係を制御部の BIND テーブル A に仮登録する．DHCP 応答を受け取ったノードは，DGW のアドレス解決を行うため，ARP 要求をブロードキャスト送信する（S211～S214）．

ARP 要求を受け取った eMLBR は，ノードがアドレス詐称していなければ eMLBR からの ARP 要求に対して ARP 応答を返すはずであることから，ARP リフレクションとして ARP 要求（ARPF 要求）をノードに送信する．ノードからの ARP 応答（ARPF 応答）を受け取った eMLBR は，応答フレーム／パケットを受信したポートをキーに BIND テーブル A を検索し，ARPF 応答の送信元 IP アドレスと送信元 MAC アドレスの対が存在しないときは，制御部の BIND テーブル A から仮登録を抹消する．一方，存在するときは接続を要求してきたノードが実在すると判定・認証し，QoS と有効期間を設定の上，転送部の BIND テーブル A に正登録する．そして，ノードからの ARP 要求（S214）に対する ARP 応答を返えす（S215～S220）．

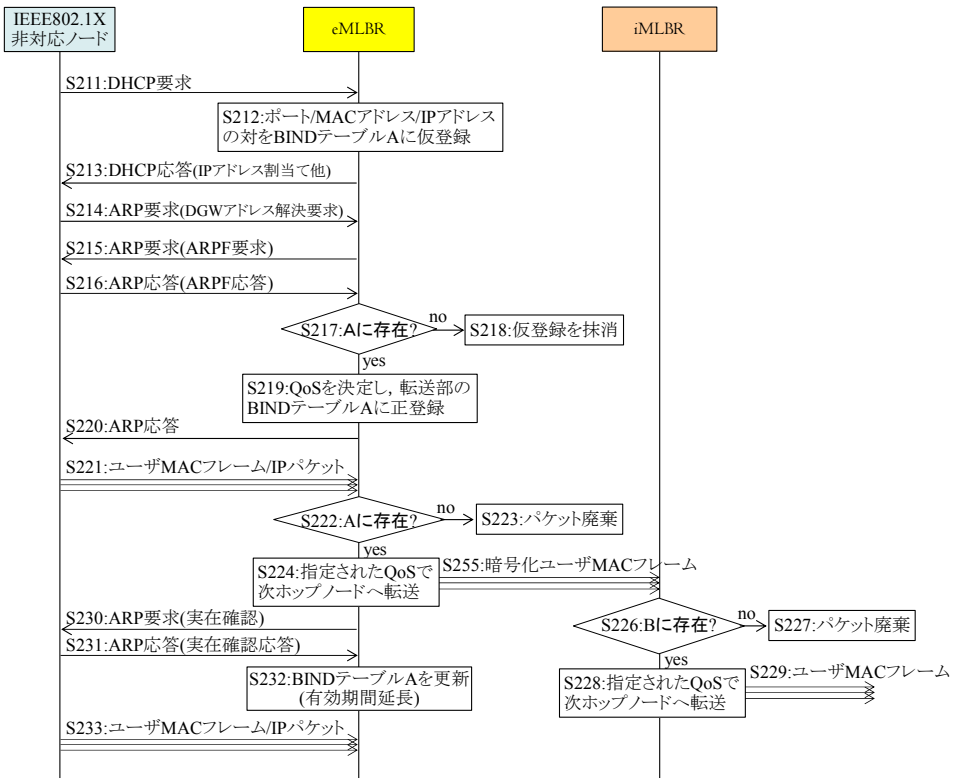


図 3　IEEE802.1X 非対応ノードの認証及びパケット転送シーケンス例
Figure 3　An example of certification for IEEE802.1X non-compliant node and sequence of packet forwarding

以後，ノードが送信したユーザ MAC フレーム／IP パケットを eMLBR が受信すると，受信したポートをキーに転送部の BIND テーブル A を検索し，送信元 IP アドレスと送信元 MAC アドレスの対が存在しないときは，同パケットを破棄する（S221～S223）．

一方，BIND テーブル A に存在するときは，指定された QoS で，またプライベート IP アドレスを割り当てた場合には eMLBR のグローバル IP アドレスに変換してから，次ホップノードである iMLBR に転送し，iMLBR でも同様の転送処理が行われる（S224～S229）．

また，eMLBR は，ノードのポートもしくはチャネルでの実在確認を適宜行い，確認結果に応じて BIND テーブル A を更新する（S230～S232）．

ARP リフレクションによる認証は，IEEE802.1X 認証より認証レベルは低い．このため，例えばテレビであれば，QoS（上り方向の帯域幅）を 10kbps に制限しても，下り方向は帯域制限しなければ，テレビの利用者はリモコン操作によるテレビ局とのデータ通信や画面の遷移に違和感を持たないと考えられる．

したがって，OS のバージョンアップやファイアウォール機能，ウィルス検知ソフトを実装していない無防備でサイバー攻撃の温床になりかねない既設のスマート家電などが，遠隔操作されて送信元 IP アドレスを攻撃ターゲットの IP アドレスに詐称して大量のパケットを送信する DRDoS 攻撃や，送信先 IP アドレスを攻撃ターゲットの IP アドレスに設定し，送信元 IP アドレスをランダムに変えながら大量のパケットを送信する SYN Flood 攻撃などに加担させられても，アドレス詐称パケットのインターネットへの大量の流出を阻止でき，たまたま端末の送信元 IP アドレスに一致した攻撃パケットだけがインターネットに流入するため，被害を最小限に抑えることができる．さらに，前述の（5）項による廃棄要請も併用すれば，攻撃パケットの長時間にわたるインターネットへの流出／流入を阻止することも可能である．

なお，本提案は MLB フィルタリング装置として，既設のルータの前段に配置することも可能である．

4. OpenFlow を用いた実装と評価実験

OpenFlow は，ネットワークスイッチの動作を制御するためのプロトコルの 1 つで，クラウドコンピューティングの負荷分散を意図に研究開発が進められている SDN（Software Defined Network）を実現する代表的な技術の一つである．OpenFlow は，制御部を担う OpenFlow コントローラ（以下，コントローラ）と転送部を担う OpenFlow スイッチ（同，スイッチ）から構成される．制御部と転送部とが一体となっている既存のネットワーク機器とは異なり，これらが分離されたアーキテクチャを採用していることが特徴である．

スイッチはコントローラに接続され，コントローラ上で動作しているソフトウェアから OpenFlow プロトコルを用いて制御される．コントローラはスイッチに対し，マッチ条件とそのアクション（処理方法）を記述したフローエントリをスイッチ内のフローテーブルへ書き込む．スイッチでは，入ってきたパケットにマッチするフローエントリを検索し，そのアクションに従ってパケットを処理する．

MLB ルータの有効性並びに実現性を検証するため、OpenFlow を用いて ARP リフレクションを適用した MLB ルータを部分試作して小規模なテストベッドを構築し，性能評価を行った．なお，より効果的・効率的に実装を行うためには，パイプライン処理によるフローテーブル間の遷移と，細かなマッチ条件の設定が必要なことから，これらの機能を併せ持つ OpenFlow 1.3 を採用した[7].

4.1 ARP リフレクションによる認証処理実験

図 4 は，試作した MLB ルータの構成と，ホスト A に対する ARPF の OpenFlow による認証処理フロー（図 3 の S214～S219 相当）を示したものである．また，表 1, 2 各々にコントローラとスイッチの機器仕様と開発フレームワークを，さらに図 5 にスイッチ内に形成されたフローテーブルの構

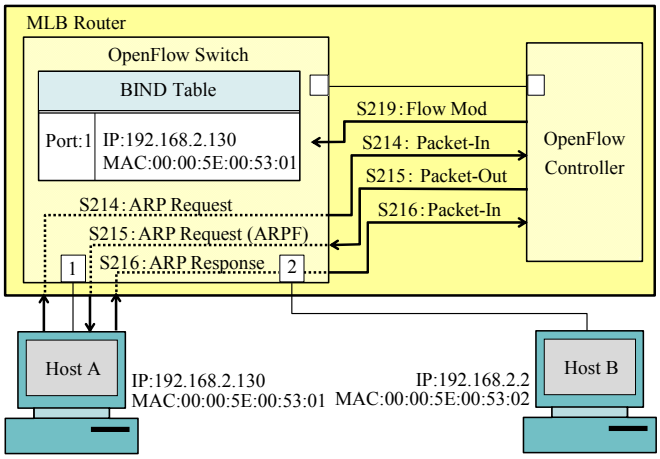


図 4　OpenFlow を用いた ARP リフレクションによる認証処理フロー

Figure 4　Certification processing flow by ARP reflection using OpenFlow

表 1　OpenFlow コントローラの概要
Table 1　Outline of OpenFlow controller

OS	Ubuntu 12.04 (x64)
CPU	Celeron 440 @2.00 Ghz
Memory	2GB
開発フレームワーク	Trema-edge [8]

表 2　OpenFlow スイッチの概要
Table 2　Outline of OpenFlow switch

OS	Ubuntu 12.04 (x64)
CPU	Celeron 440 @2.00 Ghz
Memory	2GB
開発フレームワーク	Open vSwitch [9]

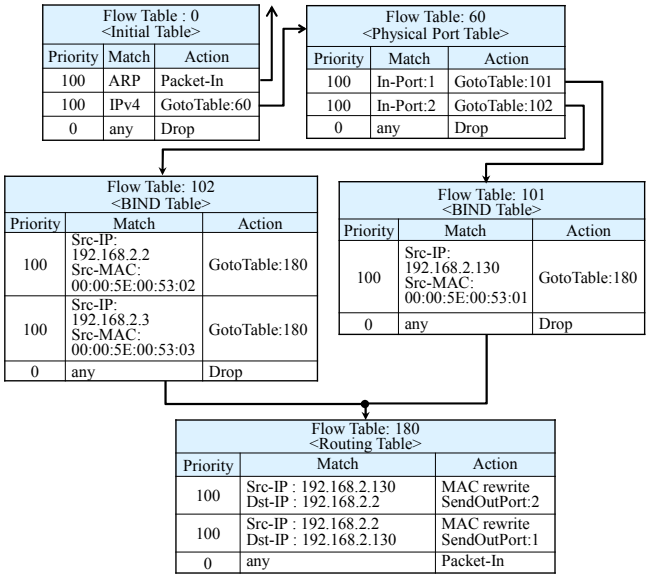


図 5　フローテーブルの構成と遷移フロー
Figure 5　Configuration of flow tables and transition flow

成と遷移フローの概要を示す. なお, ホスト A, B には DHCP によらず静的に IP アドレスを割当てた.

ホスト A が DGW を越えて通信を行おうとするとき, DGW である MBLR に対して ARP 要求を送信する. これをポート 1 で受信したスイッチは，コントローラに対して Packet-In 動作を行う（S214, Flow Table:0）. コントローラは, ARPF として, スイッチに対してホスト A への ARP 要求を Packet-Out し，スイッチはこれをポート 1 から送信する（S215）. ホスト A が ARP 応答を返すと，スイッチは再びコントローラへ Packet-In 動作を行う（S216）. コントローラは, ポート 1 をキーにホスト A からの ARP 要求（S214）の送信元 IP アドレスと送信元 MAC アドレスの対と，ARP 応答（S216）の同対とを照合し，一致していれば同対のノードが実在すると判定し認証する. コントローラはスイッチに対して Flow Mod 動作を行って（S219），“In-Port:1”をマッチ条件とするフローエントリを物理ポートテーブル（Flow Table:60）に，同対をマッチ条件とするフローエントリを BIND テーブル（Flow Table:101）に書き込む. これにより, ポート 1 に上記対以外の IP パケットが受信されたときは，廃棄されることになる.

以上の処理フローに則りホスト A がコントローラによって認証され，各フローエントリがスイッチ内の該当フローテーブルに書き込まれたことを，フローエントリ確認コマンドを用いて確認した.

さらに，外部ネットワークに接続できるようルーティングテーブルにデフォルト経路制御（0.0.0.0/0）のフローエントリを追加するなどの改良を加えた上で，テレビをインターネットに接続してみたところ，ARP リフレクションによる認証を経て，リモコン操作によりテレビ局のデータ通信サービスが利用できることを確認した.

4.2 OpenFlow を用いた MLB ルータの性能評価

(1) IP アドレス詐称パケットの遮断実験

ホスト A（機器仕様はスイッチと同じ）を攻撃者，ホスト B（OS:Windows8.1 (x64), CPU: Core i5 3317U @1.70Ghz, Memory:8GB）を被害者として，各々を 100BSAE-T でスイッチに接続し，SYN Flood 攻撃ツールを用いて送信元 IP アドレスをネットワークアドレスの範囲内（192.168.2.0/24）でランダムに詐称して，Wireshark を稼働させたホスト B に送信した.

乱数発生のシード値を変えて実験を計 6 回行った結果，ホスト B に到達できたのは，10,000 パケット中，平均して約 38 パケットであった．この約 38 パケット（≒10,000÷256）は，送信元 IP アドレスが攻撃ホスト本来の IP アドレスであった. 攻撃先に到達することができなかった約 9,962 パケットは, スイッチ上の BIND テーブル（Flow Table:101）にフローエントリが存在せず破棄されたことが，スイッチ上のログで確認できた. 以上から，本スイッチが IP アドレス詐称パケットの遮断に有効に機能することが確認できた.

(2) スイッチの性能評価実験

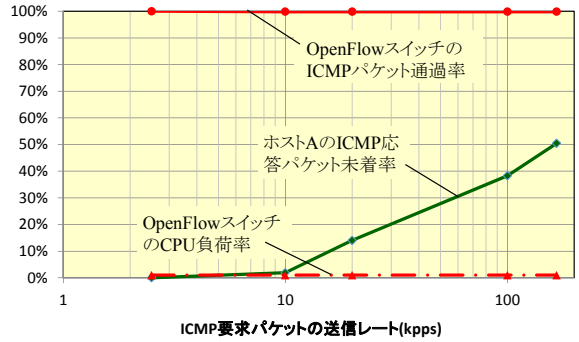
次に，フローテーブル間遷移の有無によるスイッチの性能を比較するため，パケット生成ツール hping3 を用いて，ホスト A からホスト B に対して，ICMP エコー要求パケットを，送信レートを変えて夫々10,000 パケット送信した.

図 6(A)はルーティング処理のみ, 同(B)はすべてのフローテーブルを活性化してアドレス詐称パケットの検査を加えたときのスイッチでの ICMP（要求と応答）パケットの通過率と CPU 負荷率，ホスト A での ICMP 応答パケット未着率を計測した結果を示したものである．これより，両者間に有意な差がないことがわかる.

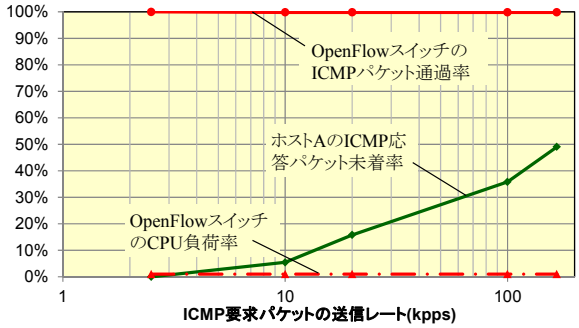
なお，ホスト B での ICMP エコー要求パケットの取りこぼしは，167kpps のときのみ約 1%観測されたが，ホスト A での ICMP 応答パケットの未着率は，送信レートが高いほど増加（167kpps のとき約 50%）している．これは，ICMP エコー要求パケットを生成・送信しながら，応答パケットの受信を行おうとするホスト A が，過負荷状態に陥り応答パケットを取りこぼしたためと考えられる．一方，スイッチでのパケットロスがなかったこと（スイッチのパケット通過率 100%）がスイッチのログから確認され，スイッチの CPU 負荷率も 1%程度と低かった.

ただし，別の実験報告[8]では．スイッチ上のフローエントリ数を大量に設定（61,000 フローエントリ）した状態で，同じポートから同じ宛先 IP アドレスに送信した場合は 143kpps 程度まで転送できたが，これらをランダムに変えながら送信した場合は 15-27kpps，また Packet-In 動作を伴う場合は 2-3kpps が限界だったとしている.

これより，ポートをマッチ条件とするフローエントリを物理ポートテーブルに，送信元 MAC 及び IP アドレスの対をマッチ条件とするフローエントリを BIND テーブルに登



(A) ルーティング処理のみ
(A) Only routing process



(B) アドレス詐称チェック+ルーティング処理
(B) Inspection of IP spoofing and routing process

図 6　フローテーブル間遷移の有無による
OpenFlow スイッチの性能比較
Figure 6　Performance comparison of OpenFlow switch between the presence or absence of flow table transitions

録し，パイプライン処理によるフローテーブル間遷移を活用してパケットの処理をスイッチ内で完結させる，すなわちマッチ条件に合致しない（アドレス詐称）パケットは Packet-In せずにスイッチ内で廃棄するなど，Packet-In の発生を最小限に抑えることが，OpenFlow を用いた MLB ルータの実装に有効なことが分かる．

5. むすび

我が国の国家予算に匹敵するほどの損害を与えているサイバー攻撃は，これまでの「自分を守ろうとするセキュリティ技術」では防ぐことは難しく，「インターネット全体での取り組み」が必要である．インターネット文化の考え方に沿い，かつ多様なポリシーのもとで運用している ISP が受け入れ得る対策案として，MLB ルータを提案した．

そのポイントは，多様なノードを対策の対象とし，認証レベルに応じて QoS を設定する，ポートまたはチャネルと送信元 MAC 及び IP アドレスとの対応関係を管理し，これから外れたパケット及び他のノードから廃棄要請されたパケットを廃棄する MLB ルータを，利用者側とインターネット側とに配備し，サイバー攻撃パケットのインターネットへの流出／流入を阻止することにある．

OpenFlow を用いて部分試作した MLB ルータを核に小規模なテストベッドを構築し，IEEE802.1X 非対応ノード対する ARP リフレクションによる認証処理，SYN Flood 攻撃に対するアドレス詐称パケットの遮断，OpenFlow スイッチの性能評価などの実験を行い，所望の機能と性能を発揮することを確認した．これらは，これまで対策のすべがなかったスマート家電への対策手段を与えるもので，その意義は大きい．また，パケット処理をスイッチ内で完結させ，Packet-In の発生を最小限に抑えることが，OpenFlow を用いた MLB ルータの実装に有効なことも述べた．

今後の課題として，IEEE802.1X 対応や，QoS 処理，他ノードから要請された攻撃パケットの遮断，IPv6 対応，実在確認などの機能実装と評価，MLB ルータへの直接的・間接的な攻撃に対する頑強性及び可用性の確保，さらに，大規模なテストベッドを構築し，様々な視点からサイバー攻撃対策としての有効性並びに既設システムとの相互接続性などを検証していくことが挙げられる．

これまでサイバー攻撃対策を強化しても，それを破ろうと巧妙化・悪質化する攻撃者とのイタチごっこが繰り返されてきた．MLB ルータは，これまでに蓄積されてきたネットワーク技術の組み合わせによって実現できる．一次プロバイダが導入を決断すれば，民間の契約ベースで対策の導入が可能である．野放し状態のサイバー攻撃を封じ，安心・安全・快適なインターネット環境をもたらし得るのか，インターネット文化や費用対効果を含めた幅広い議論を期待したい．

参考文献

1) “The economic impact of cybercrime and cyber espionage,” McAfee (2013).
URL:http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf
2) 警察庁情報通信局情報技術解析課サイバーテロ対策技術室長, “インターネット定点観測の結果と攻撃の技術的手法,” 平成 25 年度第 1 回警察政策学会情報通信研究部会, (2013).
URL:http://www.npa.go.jp/cyberpolice/material/pdf/20130709_teiten.pdf
3) P. Ferguson, D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, IETF, RFC2827, (2000).
4) IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control," IEEE Std 802.1X-2010, (2010).
URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5409813&isnumber=5409812
5) 小林浩, 江崎浩, “インターネット総論”, ISBN4-320-12039-6, 共立出版, (2002).
6) “Connected TVs, fridge help launch global cyberattack,” (2014).
URL:http://edition.cnn.com/2014/01/17/tech/gaming-gadgets/attack-appliances-fridge/
7) “OpenFlow Switch Specification Version 1.3.1,” The Open Networking Foundation, (2013).
URL:https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.1.pdf
8) “Trema,” (2013). URL:http://trema.github.io/trema/
9) “Open vSwitch,” (2013). URL:http://openvswitch.org/
10) Hiroki Ide, “OpenFlow スイッチとしての Open vSwitch の性能,” (2013).
URL:http://bird-blog.bit-isle.co.jp/2013/08/openflow-open-vswitch.html