社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＭＢＬ－29　(28)
2004／5／14

Mobile IPv6 環境下における 認証型ファイアーウォールに関する検討

山田 勇二　小出 和秀　北形 元　白鳥 則郎

東北大学大学院情報科学研究科/電気通信研究所

〒980-8577 仙台市青葉区片平 2-1-1

E-mail: {yuji,koide,minatsu,norio}@shiratori.rice.tohoku.ac.jp

あらまし　本稿では，Mobile IPv6 環境下におけるファイアーウォールに起因する問題を解決するシステムとして，認証型ファイアーウォールの提案，検討を行なう．認証型ファイアーウォールは Mobile Node が移動した先のネットワークでファイアーウォールやセキュリティポリシーの違いにより Binding Update が失敗してしまう問題を解決するものである．本稿では，動的に設定を変更する認証型ファイアーウォールシステムの構成を提案し，検討を行なう

キーワード　Mobile IPv6，認証型ファイアーウォール，Hierarchical Mobile IPv6

A Study on the authenticated type firewall under Mobile IPv6 environment

Yuji YAMADA　Kazuhide KOIDE　Gen KITAGATA　and　Norio SHIRATORI

Research Institute of Electrical Communication/Graduate School of Information Science,

Tohoku University, 2-1-1 Katahira Aoba-ku, Sendai, 980-8577,JAPAN.

E-mail: {yuji,koide,minatsu,norio}@shiratori.rice.tohoku.ac.jp

Abstract　In this paper we proposed an authenticated type firewall and examine it as a system that can solve the firewall problem under Mobile IPv6 environment. When a Mobile Node moves from one network to another, the binding update fails due to the difference in security policy or firewall of the new network. This paper describes a dynamic system configuration technique of an authenticated type firewall that can overcome this problem.

Keyword　Mobile IPv6, authenticated type firewall, Hierarchical Mobile IPv6

1. はじめに

近年，ノート PC や携帯型端末（PDA）などの普及や，無線 LAN インフラの充実により，インターネット輪に代表される IP ネットワーク上で提供されるサービスを受けながらネットワークを移動した際に，そのサービスを継続して利用したいという要求が高まっている．この要求を満足する一つの解決法として，これに答えるものとして Mobile IPv6(MIPv6)が提案されている[1].

1.1. Mobile IPv6

Mobile IPv6 の目的は，端末がネットワークのどこに接続しても，また移動を続けながらでも，同一の IP アドレスを保ったまま，間断なく通信を継続できる環境を提供することにある．これを実現する手順を Fig.1 に示す．Mobile IPv6（以降 MIPv6 と表記）では，移動するノードである Mobile Node（以降 MN と略記）は必ずホームネットワークに所属し，このホームネットワークで使用する Home Address が割り当てられる．MN がネットワークを移動すると移動先の Router から Router Advertisement(RA)を受け取り，Care-of Address を生成し，この Home Address と Care-of Address のペアからなる情報をホームネットワーク上にある Home Agent(以降 HA と略記)に Binding Update(以降 BU と略記)を送信することで通知する．これにより MN の Home Address と Care-of Address との対応付けがなされ．MN の通信相手である Correspondent Node(以降 CN と略記)から Home Address 宛てに届くパケットを HA がこの対応付けを利用して MN に対して転送を行なうことができるようになる．この結果，MN はネットワー

クを移動しても，同じ IP アドレスで通信を継続することができる．

さらに HA でこの対応付けが完了した後，次に MN は CN に対しても同じように，Home Address と Care-of Address との対応付けを行なうことができる．その結果，CN から MN 宛てに届くパケットを HA 経由ではなく，最適化された経路，すなわち CN から MN への直接経路を通って送受信が可能になる．このように MIPv6 では，Home Address と Care-of Address との対応付けを利用することで，同一アドレスでの接続を維持している．

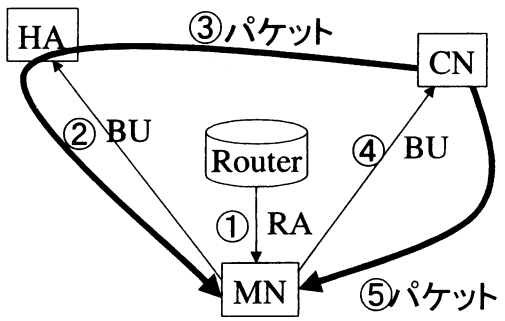

Fig.1 Binding Update の手順

1.2. MIPv6利用上での問題

MIPv6 では MN から送信される BU が HA に届かなかった場合，接続性を維持することが出来なくなってしまう．また，たとえ成功したとしても，セキュリティポリシーの違うネットワーク間を移動した場合，移動前のネットワークで利用できていたアプリケーションが，移動後のネットワークでは利用できなくなるという問題が発生してしまう．この場合，全てのパケットを HA から MN へのトンネル経由で MN に届けることで，アプリケーションの利用は可能になる．しかし，HA を経由させることで，高い確率で遅延が発生し，アプリケーションの実行に支障をきたしてしまう．このような問題の多くは，移動先のネットワークにあるファイアーウォール(以降 FW と略記)に起因している場合が多い．

FW の多くは外部ネットワークから内部ネットワークに流れるパケットのフィルタリング目的で設置されている．また内部ネットワークから外部ネットワークに流れるパケットの制限も行っている．内部から外部へのフィルタリングの目的は，管理者側で策定されたセキュリティポリシーに従い，利用可能なサービスや外部ネットワークへのアクセス制限などを行なうためである．この点が MIPv6 において問題になる．

MIPv6 では，ネットワークを移動した先で生成される Care-of Address を用いて，実際の通信を行っている．移動先のネットワークにある FW が，この Care-of Address によるアクセスを制限していた場合，Fig.2 に示すとおり，移動した MN は HA に対して Home Address と Care-of Address の対応付けの更新ができず，Home Address での接続を維持できなくなってしまう．また仮に HA で対応付け表が更新された場合でも，MN に対して更新ができたことを通知する Binding Acknowledgement(以降 BA と略記)が FW によって遮断された場合，同じように接続を維持できなくなる．

また Fig.3 に示すとおり，移動先ネットワークのセキュリティポリシーにより，アプリケーションの利用が，そのネットワークをホームネットワークとしているノードのみに利用が制限されてしまうことが考えられる．Fig .3 にその図を示す．

本稿では 2 章で FW に関する問題，3 章で提案システム，4 章で提案システムの検討，5 章で結論について述べる．

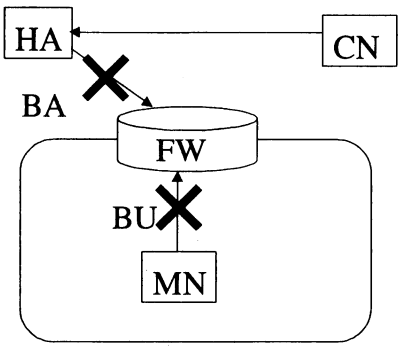

Fig.2 BU 失敗が失敗する場合

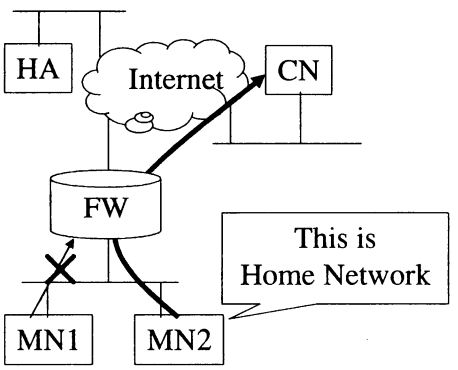

Fig.3　セキュリティポリシーに関する問題

2. FW に関する問題

FW は，セキュリティ向上の観点から，外部ネットワークから内部ネットワーク，又は内部ネットワークから外部ネットワークへのアクセス制限を目的として設置されている．これはネットワークの利用を無制限に行なえるようにしたくないという管理者側の要求に基づくものである．このことからも現実のネットワークで FW の存在を無視することはできない．そして，移動先のネットワークにある FW が，MN の外部へのアクセスを制限してしまい，HA への BU やアプリケーションの利用の妨げになる可能性がある．この場合，MIPv6 環境を構築する上で，この FW が MIPv6 の利用を妨げる障害になってしまう．

この問題は，一般的に FW がセキュリティポリシーに基づき静的に設定されているため，MN のような外部ユーザに対して動的に設定を変更することが困難であることに起因する．またセキュリティ上，なんの認証もせずにネットワーク利用を行なえるようにしたくないという，管理者側の考えもこの問題の原因となっている．この問題を解決するためには，ネットワークを利用する外部ノードに対して，なんらかの認証を行い，FW の設定を動的に変更し，ネットワークの利用を開始させることが必要である．本研究ではこれまで述べたような FW によって，内部から外部へのアクセス制限が行なわれているネットワークを想定する．

2.1. 既存の認証システム

前述の問題を解決する既存システムには Gateway と認証サーバが連係してネットワークの利用許可／拒否を決定する認証システムが多く，これらのシステムのほとんどは Gateway が FW を兼ねている．具体的な既存のシステムとして Opengate[2]や authipgate[3]，PortGuard[4]などがある．例として，Opengate システムを Fig.4 に示す．

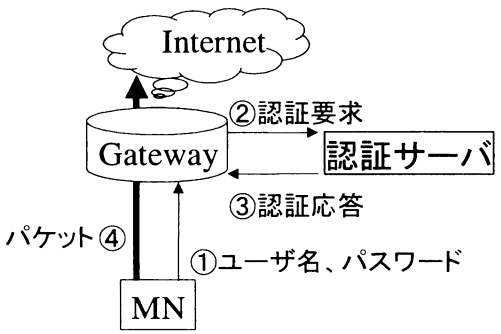

Fig.4 Opengate の動作

この認証システムでは，ネットワークを利用するユーザは，まずユーザ名とパスワードを Gateway へ通知する．この通知を受け取った Gateway では，認証サーバに対して，ユーザ名とパスワードによる認証要求を出す．認証サーバでは，ユーザ名とパスワードによる認証を行い，認証結果を Gateway へ認証応答として通知する．Gateway では，認証結果に基づき，認証が成功していた場合，ネットワークの利用を許可する．認証が失敗していた場合，ネットワークの利用を拒否する．この認証システムでは，認証がユーザ名とパスワードで行なわれているために，ユーザ名とパスワードの事前登録が必須になっている．この事前登録はユーザにとって，負担である．さらに接続するネットワークを管理する組織が大学や会社など異なる場合，一つ一つの組織に対して認証に必要な情報を登録することは，現実的ではない．また管理する側から考えた場合，ユーザ情報の登録や管理は大きな負担となる．さらに MIPv6 環境を考えた場合，ネットワークを移動するたびにパスワードを入力していたのでは，ハンドオーバにかかる時間が増加してしまい，アプリケーションレイアなどの上位レイヤに大きな影響を与えてしまう．

3. 提案システム

本章では Hierarchical Mobile IPv6[3]の仕組みを活用し，動的に設定が変更可能な認証型 FW を提案する．

3.1. Hierarchical Mobile IPv6

Hierarchical Mobile IPv6（以降 HMIPv6 と表記）の目的は，同一ドメイン内でのハンドオーバを効率化することである．そのために，外部ネットワークと外部ネットワークの境界に Mobility Anchor Point(以降 MAP と略記)を置き，MAP において MN の Home Address と Care-of Address を管理することでハンドオーバの効率化を実現している．

シグナリングの流れを Fig.5 に示す．

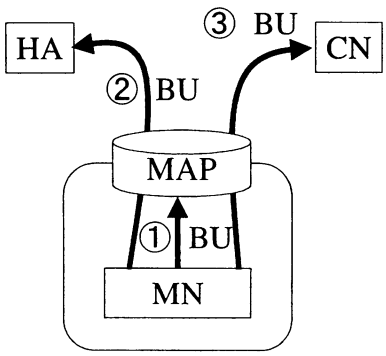

Fig.5 HMIPv6

MN は MAP が設置されているネットワークに接続すると，MIPv6 と同様に Care-of Address を生成する．MIPv6 では HA に対して BU を送信するが，HMIPv6 では MAP に対して BU を送信する．これにより，MAP には MN の Home Address と Care-of Address の対応付けが作成される．次に MN は HA，CN に対して Home Address と Care-of Address の対応付けを行なう．以上で最初の Home Address と Care-of Address の対応付けが終わる．この段階では通常の MIPv6 よりシグナリングコストがかかっているので，ハンドオーバタイムは大きくなる．

しかし，この後同一ドメイン内の別のセグメントのネットワークに移動した場合，新しく生成される Care-of Address の BU は MAP に送信すればよいので，HA や CN には送信しないで済む．これにより，Home Address と Care-of Address の対応付けの更新に必要な時間を短縮することで，MIPv6 よりも早く通信を再開できるようになっている．

3.2. 認証型 FW：A-FW

本章では，HMIPv6 の実装されている環境を想定し，HMIPv6 の仕組みを活用した認証型 FW (Authentication-FireWall:以降 A-FW と表記)システムを提案する．このシステムは HMIPv6 のシグナリングを用いて MN を認証し，その認証結果からネットワークの利用に対する許可，又は拒否を決定する．ネットワークの利用を許可した場合，該当 MN に対して FW を開放し，またその MN が違うドメインのネットワークに移動した場合，FW を閉めるというものである．A-FW システムは MAP，FW，MN 管理機構，FW 制御機構によって構成される．Fig.6 に A-FW のシステム構成を示す．

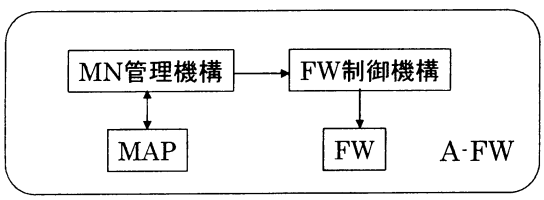

Fig.6　A-FW のシステム構成

3.2.1. MN 管理機構

MN 管理機構には MN 認証機能，MN 接続確認機能の二つの機能がある．

まず MN 認証機能について説明する．MN の認証は HMIPv6 のシグナリングを用いて行なう．MN の認証は HA で行ない，A-FW では MAP に生成される Home Address と Care-of Address の対応付け表（以降，Home Address と Care-of Address の対応付け表を対応付け表を表記）と，HA から MN へ対応付け表が作成されたことを通知する BA により，認証の成功／失敗を判断する．また本機構では，MAP において対応付け表が完成したことと，認証結果を FW 制御機構へ通知する作業も行なう．

A-FW では認証機能により，MN の Home Address と Care-of Address の対応付け，ホームネットワーク，HA の IP アドレスを得ることができる．これらの情報は，セキュリティ対策として，取得することで，MN が不正行為などを行なった場合に，用いることができると考えられる．また HMIPv6 のシグナリングをそのまま利用していることから，新たな認証手続きを踏むことなく利用できるメリットがある．

次に MN 接続確認機能について説明する．この機能は，MN が MAP が存在するネットワークに現在接続しているか，していないかを確認するものである．すなわち，接続状況を確認することで，MN が別のネットワークに移動したのか，していないのかを判断するものである．この機能の目的は，MN が別のネットワークに移動したにもかかわらず，FW を開放したままになるのを防ぐことである．

HMIPv6 のシグナリングにより，MAP に MN の対応付け表が作成され，この表には有効期限が設定されている．MN は別のドメインのネットワークに移動しない限り，この有効期限が切れる前に，再び MAP に対して BU の送信を行なう．すなわち，MN が同一ドメイン内にいる間は，MAP に作成される MN の対応付け表は維持される．有効期限が切れるとこの表は削除される．そこで，この表が存在するか，しないかを確認することで，MN の接続を確認する．ＭＮ認証機能とＭＮ接続確認機能の動作を Fig.7 に示す．

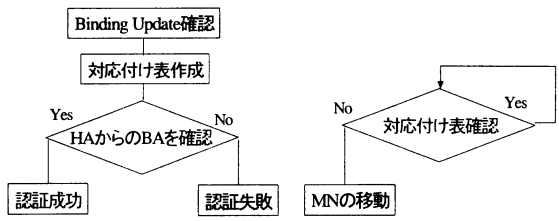

Fig.7　MN 認証機能と接続確認機能の動作

3.2.2. FW 制御機構

この機構では MN 管理機構によって通知される認証結果，MN の移動通知，MAP への対応付け表作成に関する情報に基づいて，①～③の手続きで FW の設定を変更する．

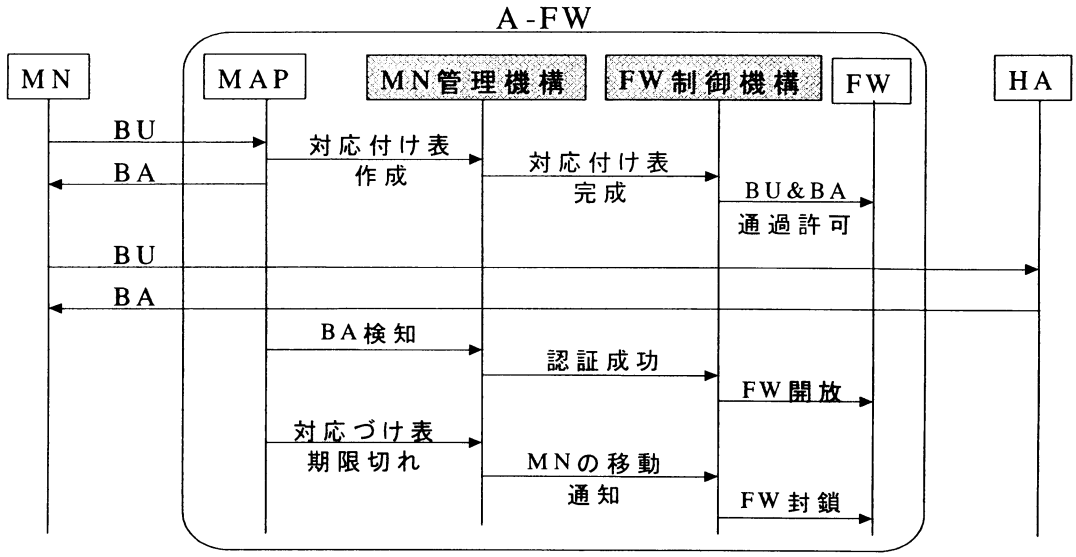

Fig.8　A-FW システムの動作

Table.1　検討結果

	認証にかかるコスト	事前登録の必要性	設置可能箇所
Opengate	大	有り	制限無し
提案システム	小	無し	制限あり

① MAP 内に対応付け表が作成されたことが通知された場合，HA への BU と MN への BA が通過できるように FW を開放する．
② 認証の成功が通知された場合，FW を MN に対して開放する．
③ 接続が切れたことを通知された場合，FW を閉じる．

このように FW の設定を変更することで，MN のアクセス制御を活用して，動的に制御する．

3.2.3. A-FW の動作

本システムの具体的な動作は以下のようになる．

① MN から MAP 宛ての BU を受信
② BU を受け取った MAP は MN の Home Address と Care-of Address の対応付け表を作成
③ MN 管理機構は Home Address からホームネットワークを判断し，HA への BU の送信を許可するように FW 制御機構へ対応付け表の完成を通知
④ HA への BU と BA が通過できるように FW を開放
⑤ MN は HA に対しても BU を送信
⑥ HA では対応付けの作成が成功したことを表す BA を送信
⑦ MN 管理機構は MAP において HA からの BA を確認し，認証の成功を FW 制御機構に通知
⑧ 通知を受けた FW 制御機構では MN に対して FW を開放
⑨ MN 管理機構は MAP 内の対応付け表を監視
⑩ MN 管理機構は MAP 内の対応表から MN の対応付けが削除されたのを確認し，FW 制御機構に MN の接続が切れ移動したことを通知
⑪ 通知を受けた FW 制御機構が FW を閉じる

ここで，HA のなりすましを防ぐ方法として，③において信頼性があるホームネットワークだけに接続を許可するようにすることが考えられる．信頼のおける HA への対応付けのみを許可することで，自宅など不特定な HA への対応付けを防ぐことができる．これにより，認証の正当性を向上できる．

4. 検討

本システムの利点と欠点について検討する．まず利点として，認証機構に HMIPv6 のシグナリングをそのまま利用しているため，既存のシステムで行なわれているようなパスワードなどによる認証手順を必要としない．これにより認証にかかるコストを少なくできる．さらに，パスワードなどユーザ情報の事前登録を必要としないことより，動的にユーザの認証を行なえると考えられる．この結果，ネットワークの管理者側では，ユーザの情報の管理や認証サーバを設置する必要がなくなり．管理者の負担を軽減できる．

次に欠点として，HMIPv6 の導入が前提になるため，システムの設置にあたって，ネットワーク構成による制限が生じる場合がある．ただし，HMIPv6 はハンドオーバの効率化を目的として提案されたものであり，リアルタイムアプリケーションの利用を考えた場合，今後一般に広く利用される可能性は大きい．以上の検討結果を Table. 1 にまとめる．

既存のシステムは MN のような外部ノードが，ネットワークを利用するような環境を想定して構築されていない．さらに認証に事前登録を必要とするなど，ユーザ，管理者側の双方で手間が発生してしまう．これに対して，本システムではこれらの手間を解消する．さらに，本システムは既存の HMIPv6 に特別な変更を行なわずに，導入することが可能であり，加えて，既存の MN，HA，CN もそのまま利用可能である．よって，既存システムとの親和性が高いシステムである．

5. 結論

本研究では動的に設定が変更可能な認証型 FW を提案し，システムの利点欠点について検討した．その結果，本システムは FW に起因する問題の解決に有効であることを示した．

本稿では移動した先のネットワークの FW に関する問題を解決した．今後は，CN が接続しているネットワークにある FW（外部の FW）に関して，検討を行っていく．

文　献

[1] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-24.txt, June, 2003.

[2] Opengate: http://www.cc.saga-u.ac.jp/opengate/

[3] authipgate:http://www.sc.isc.tohoku.ac.jp/~hgot/sources/authipgate.html

[4] PortGuard:http://www.portguard.org/

[5] H. Soliman, C. Castelluccia, K. E. Malki and L. Bellier , "Hierarchical Mobile IPv6 mobility management," draft-ietf-mipshop-hmipv6-01.txt, Feb, 2004.