マルチメディア通信と分散処理　94－24
分散システム／インターネット運用技術　14－24
（１９９９．７．１６）

既存のDHCP端末で利用できる 利用者にも管理者にも安全な情報コンセントシステムの構築

丸山　伸†，浅野善男‡，辻　斉†，藤井康雄†，中村順一†
†京都大学　総合情報メディアセンター
‡立命館大学　理工学研究科

概要

情報コンセントを運用する際に用いられるDHCPには認証機構やセキュリティ対策に関する内容は含まれていない．そのため，不特定多数が利用する環境においてセキュリティを保持しようと考えた場合，その実現は非常に困難であった．
本論文では，既存のDHCPおよびそれを利用するクライアント環境に変更を加えることなく情報コンセントに対して認証機構を導入し，同時にセキュリティの向上を行う方法を示す．また，同環境の運用から得られた経験についても述べる．

A secure LAN sockets system for everyone which need not modify existing DHCP clients

Shin Maruyama †, Yoshio Asano ‡, Hitoshi Tsuji †, Yasuo Fujii †, Jun-ichi Nakamura †
†Center for Information and Multimedia Studies (CIMS), Kyoto University
‡Graduate School of Science and Engineering, Ritsumeikan University

Abstract

DHCP, which is used when we provide LAN socket with network accessibility, include neither authenticate mechanism nor measures against security. Therefore, it is very hard to give this kind of service to public with keeping security.
In this paper, we will show a way of providing LAN socket with both authenticate mechanism and improvement in security without modifying both DHCP and DHCP client software. We also show our experience which is acquired through managing LAN socket of this kind.

1．はじめに

情報コンセントは，機器を接続するだけで自動的にIPアドレスが割り振られ，ネットワークに接続できるという利便性を目的としている．そのためか自動的にIPアドレスを割り振るためのプロトコルであるDHCP[1]には，利用者を認証するための機構は含まれていない．また，接続する端末や接続されるネットワークのセキュリティの維持や向上を目的とする機構も含まれていない．

このプロトコルを利用する上で発生するセキュリティ上の問題点は早くから指摘されている．また，様々な改良法が提案されている．DHCPに認証機構を追加しようという動きもある[2]がその実装はクライアントに変更を強いるものである．すでに既存のDHCPクライアントが普及している現状において，急なプロトコル変更が実現できるとは考えにくい．

そこで我々はいくつかの既存の技術を効果的に組み合わせることで，DHCPに変更を加

えることなく，利用者を認証するため機構とセキュリティの向上を図った情報コンセントシステムの設計と実装を行った．

本論文では，情報コンセントの設置における技術的問題点を明確にするとともに，従来のDHCPには含まれていない「認証機構」と「セキュリティの向上」を既存のDHCPクライアントで如何に実現したかについて述べる．また，本システムの運用から得られた経験を紹介する．

2. これまでの情報コンセントの問題点

2.1. 利用状況が不明確

これまでの情報コンセントは，接続するだけで利用できるように設定されているため，情報コンセントの利用状況を知ることができない．

教育環境のような場所で不特定多数に対して情報コンセントを公開する場合，“いつ”，“だれ”が，“どの情報コンセント”で利用したかという記録を残す必要がある．この問題を解決するには，DHCPによる接続の過程の中で，認証を行い利用者名を特定する機構を準備する必要がある．

2.2. 利用者端末への攻撃

情報コンセントに接続される端末は，利用者の個人端末である可能性が高い．そのような端末は外部からの攻撃に対して弱いことが予測されるため，管理者にとって利用者の端末のセキュリティを守ることも運用上重要となる．また，DHCPはその実装上の理由によりARPブロードキャストを利用する．そのため複数の利用者端末を接続することが可能な環境を用意した場合，その複数の端末は同一のネットワークに置かれることが多く，相互に通信を行うことが容易である．そのため，利用者端末のセキュリティを守るためには，外部からの攻撃を防ぐだけではなく，情報コンセントの利用者間での攻撃を防ぐことも重要となる．

2.3. 外部アクセスに対するアクセス制御

情報コンセントの利用記録をとるだけでは，たとえ認証機構を設けたとしても，完全に安全になったとはいえない．特に，不特定多数に対して情報コンセントを公開する場合，各情報コンセントから外部ネットワークへのアクセス制御は重要である．利用できるサービスを限定させるためにも，第3層以上でのアクセス制御ができることが望ましい．

3. これまでのDHCPの拡張例

これまでに述べたような問題点を解決するためにこれまでにいくつかの試みが行われてきた．それをここに紹介する．

3.1. 山口大学における実装例[3]

ゲートウェイを設置して外部との接続を遮断する方法を用いている．認証を通過することで外部との接続が可能となる．しかし，クライアント同士の通信は自由にできることで，セキュリティ的には問題があるといえる．

3.2. 大阪市立大学における実装例[4]

IPの成りすましなどの対策などを行っている．またスイッチングハブにおいてポート単位のセキュリティをかけるなどの点においてもセキュリティに配慮がなされている．ただし，クライアント側に専用のソフトウェアーが必要であるため，情報コンセントの利便性が損なわれている．

3.3. internet-draft における DHCP の拡張案[2]

DHCP に認証を追加するための機能拡張をしようという動きがある．サーバだけでなくクライアントの変更も必要となる．

4. 本論文における DHCP の拡張

4.1. 目標

本論文では従来より広く使われている DHCP に運用上の工夫を設けることにより次の特徴を備えるようにすることを目標とする．

- 特定のアカウント名とパスワードによって認証されない限り，外部へのアクセスを禁止する．(管理者にとって安全)
- あるクライアントがサーバから受け取った IP アドレスは，MAC アドレスと情報コンセントを変更しない限り有効である．(管理者にとって安全)
- 外部ネットワークからクライアントに対する接続を拒否する．(利用者にとって安全)
- クライアント相互間での通信を禁止する．(利用者にとって安全)
- クライアントとサーバ間の通信を他のクライアントから傍受されないようにする．(利用者にとって安全)
- 既存の DHCP クライアントを利用し，クライアント側に拡張を加えない．
- 認証には Web ブラウザによる CGI のみを用いる．

4.2. 実現に利用した既存技術

本論文における DHCP の拡張で用いた既存技術をどのように利用したかを述べる．

4.2.1. VLAN

情報コンセント間で ARP ブロードキャストが流れるのを防ぐために，各情報コンセントを VLAN により分離した．また，サーバはこれらすべての VLAN に属し，どのクライアントとも通信ができる必要がある．よって，サーバとスイッチングハブ間を Muliti VLAN に設定し，そこにすべて VLAN を割り当てた．サーバおよびスイッチングハブの機種依存性をおさえるために，Cisco の提案による ISCP によるものではなく，IEEE802.1Q に従った VLAN の実装を利用するのが望ましい．サーバ側で VLAN の区別ができるため，より安全である．

4.2.2. MAC アドレスの偽造防止

一度認証が行われた後，その IP アドレスを利用して別のクライアントが通信を行えるようなことがあってはならない．この対策として，スイッチングハブで MAC Filtering をすることにより回避する．ただし，同一情報コンセントかつ同一 MAC アドレスからアクセスを通過させてしまうため，端末が入れ代わらないように接続確認を十分に頻繁に行う．また，スイッチングハブからの Link Down シグナルをトラップする方法も考えられる．

4.2.3. NAT

外部からクライアントに対する直接の攻撃を防ぐ効果的な方法のひとつとして，クライアントの IP アドレスを外部に見せないことがあげられる．外部からのコネクションを張れないという NAT の欠点ともなりうる点を逆に利用し，外部ネットワークからのアクセスを拒否するために利用する．

4.2.4. IP Forwarding

情報コンセントの利用者にとって，認証を行うための手続きは出来る限り簡便なものであることが望ましい．本論文における実装においては認証に Web ブラウザを通して CGI

を起動させる方法を用いた．各クライアントがDHCPによってIPアドレスを取得した後，ブラウザを起動した際に「スタートページ」を取得する．その際のパケットを横取りし，認証Webサーバに転送することにより，実際にはそのパケットをスタートページの示すサーバに届けることなく，認証を行うCGIの内容に差し替えてクライアントに応答する．

これにより，ユーザは認証を行うための設定を特別に行わなくとも，管理者の想定している認証システムに接続することが可能となる．

4.2.5. DHCP Requestに対する応答パケットのSniffing対策

DHCP Requestに対する応答パケットがARPブロードキャストパケットによってサーバーから送出されるような実装になっていると,スイッチの実装によってはそのパケットをSniffingされる可能性がある．そのため応答パケットはブロードキャストではなく特定のMACアドレスに向けて送出されなければならない．また，そのパケットがクライアントにまで流れないようにするため,スイッチングハブの各ポートは自分の下流にあるMACアドレスを記憶しそこに含まれないDestinationをもったパケットはForwardingしないようにするセキュリティ機構を備えていなければならない．

4.3. システムの全体構成

本システムは次のような構成となっている．

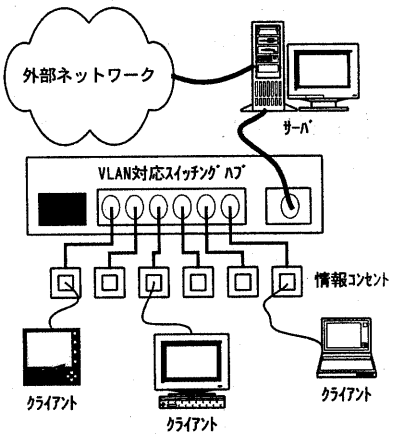

図1．システム構成図

4.3.1.サーバ

サーバでは以下の機能を受け持つ．

- DHCPサーバ(IPアドレスの配布)
- Webサーバ(認証ページ用，監視ページ用)
- DNSサーバ(queryの中継用)
- 認証サーバ(本研究ではNISを利用)
- 接続監視サーバ(クライアントの監視)
- IP Filtering
- NAT

サーバは次のような状態遷移をする．(図2)

① 待機状態
② DHCPによるIPアドレスの付与
③ CGIによる認証要求を待つ
④ NISでユーザ名及びパスワードを確認
(成功→⑤，失敗→③)
⑤ IP Filteringで外部アクセスを許可
⑥ クライアントの接続確認
(成功→⑥，失敗→⑦)
⑦ IPアドレスの強制開放
⑧ ①にもどる

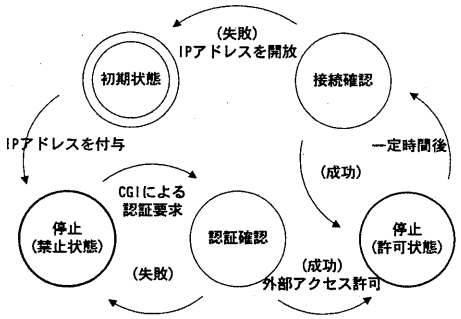

図2．サーバの状態遷移図

4.3.2. クライアント

クライアントは最低限以下の機能を持つが必要である．いずれも広く使われている機能であるため，この制限が問題となる事は少ないと考えられる．

・DHCP クライアント

・Web ブラウザ

利用者は次のような操作を行う．(図 3)

① DHCP によるアドレスの取得

② Web ページ上での CGI による認証

③ IP アドレスの解放

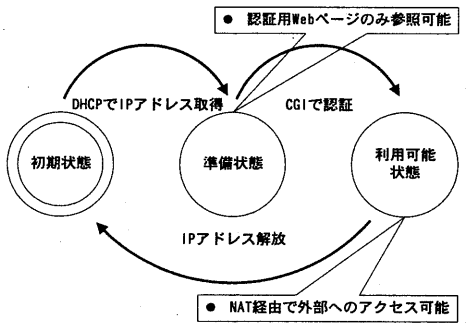

図3．端末の状態遷移図

4.3.3. スイッチングハブ

スイッチングハブは以下の機能が備わったものを利用する．

・VLAN の設定ができる．

・単一ポートに複数の VLAN が設定できる．(MultiVLAN, IEEE802.1Q trunk 等)

・MAC Filtering

5. 評価

実際に図書館に情報コンセントをサービスするシステムを構築し運用した．ハードウェアおよびソフトウェアは以下のものを用いた．

Hardware:	Cisco Catalyist2912-EN
	AT 互換機(自作)
OS:	FreeBSD-3.1
DHCP サーバ:	ISC-DHCP2.b1.6
Web サーバ:	Apache-1.3.4
DNS サーバ:	Bind-8.1.2
認証サーバ:	OS 付属の NIS
接続監視サーバ:	perl による daemon を作成
IPFiltering:	OS 付属の IPFW
NAT:	OS 付属の NATD

運用をする中で得られた経験として次のような問題があった．

・Microsoft 製 Internet Explorer を利用しているユーザが認証を正常に行えない．これは Microsoft 製 Internet Explorer が Expire を規定どおりに行わず，内部にキャッシュを保持しつづけることによる問題であった．これに対する対策のため，認証スクリプトにおける Last Modified ヘッダの内容を毎回更新するようにした．

・FTP アクセス等によりアップリンクの帯域占有される場合に，周囲のユーザーの帯域が圧迫されることがあった．可能であれば各クライアント毎の帯域制御が行えるようになっていることが求められるかもしれない．

このような問題はあったものの，概ね利用者にとって快適にこのサービスを提供できている．

6. おわりに

本論文では，管理者と利用者の両者にとっての安全性および利便性を考慮した情報コンセントシステムを提案した．とりたてて目新しい技術はないものの，既存の技術をうまく使う事により本システムが構築できたものと考えている．セキュリティが重要視される中，意外に身近なところに問題が存在し，そして抜け道もまた潜んでいる．それらの問題に対し適切に対処をすることで，より利用しやすい環境が実現できると思われる．

参考文献

[1] R.Droms: "Dynamic Host Configuration Protocol", RFC 2131. 1997.

[2] R.Droms, W.Arbaugh: "Authentication for DHCP Messages", draft-ietf-dhc-authentication-10.txt, Internet Draft, 1999.

[3] 久長，岡田，刈谷: "情報コンセントに接続された計算機に対するMACアドレス/IPアドレスの偽造防止手法"，情報処理学会コンピュータセキュリティ研究会コンピュータセキュリティシンポジウム'98論文集, pp.141-146, 1998.

[4] 石橋，山井，阿部，大西，松浦: " 情報コンセントにおける認証と MAC アドレス/IP アドレスの偽造防止を実現するシステム LANA の設計と実現" ，情報処理学会分散システム/インターネット運用技術研究会分散システム/インターネット運用技術シンポジウム'99 論文集，pp.69-74, 1999.