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

2006－DPS－127 (6)
2006／6／5

DHCPサーバを用いた利用者管理システムの提案

乃村能成† 入江正博†† 谷口秀夫†

オフィスのLAN環境において，接続計算機の利用責任者，所在，使用IPアドレス，MACアドレス，導入済ソフトウェアなどを厳格に管理することが求められている．これは，情報漏洩防止，著作権保護が叫ばれる中，小規模なオフィスや教育機関も例外ではない．これらのオフィスにおける管理状況は様々である．例えば，管理の容易さからDHCPサーバを介して自由に計算機の接続を許している所もあれば，利用者に申請書の提出を求めて，厳格な台帳管理を実施している所まで幅がある．前者は，障害対応が困難になる問題以外に，外部に対する説明責任という観点からも問題がある．後者は，台帳と現状の同期を維持することが難しい．本稿では，利用者に3つのクラスを設け，そのクラスに応じたIPアドレスをDHCPサーバが付与する方式を提案する．これによりIPアドレスベースの利用制限をしつつ，利用者自身で管理台帳を更新するように誘導する．

A User Management System Using DHCP Server

YOSHINARI NOMURA,† MASAHIRO IRIE†† and HIDEO TANIGUCHI†

Recently, we are supposed to manage information about all PCs in every office, such as administrator, location, mac-address, list of installed softwares... However, it is difficult to do that strictly, some sites give up the management and a DHCP server supplies a free-to-connect network inside the LAN. Besides security risks, the situation is ugly. That is, we have to be accountable for compliance with laws: information leakage protection, software license management. In this paper, we describe a system to help changing the situation gradually. We introduce IP address based classify of users using DHCP server. It is naturally acceptable to free-to-connect network. This IP address based restriction gradually lead users to manage their PCs by themselves.

1. はじめに

計算機の低価格化と同時に安価なファイヤーウォール装置の出現によって，企業の1つの部署や大学の研究室単位でも比較的小規模なプライベートネットワーク(以下，固有網)を構築可能になっている．一方，情報漏洩防止，著作権保護が叫ばれる中で，ネットワーク環境に接続している計算機の利用責任者，所在，使用IPアドレス，MACアドレス，導入済ソフトウェアなどを厳格に管理することが求められている．これは，小規模な固有網においても例外ではない．

これらの固有網における計算機管理方針は様々である．例えば，管理の容易さから，DHCPサーバを介して自由に計算機のネットワーク接続を許している固有網もあれば，利用者に利用申請書の提出を求めて，厳格な台帳管理を実施している固有網もある．両者の間に幅があるのは，前者の緩やかな管理方針であっても，ネットワークの使い勝手という観点からは，それほど問題にならない場合が多いためである．つまり，固有網は小規模で，機器の所在の分散は小さく，外部からも分離されているため，障害発生時に限って人手をかければ事が足りるためである．もちろん，後者の方針を採用し，台帳によって計算機情報を厳格に管理しておけば，障害対応はいくらか迅速になる可能性はある．しかし，それによるメリットに比べて，台帳管理のコストは高く，利便性の観点から積極的に採用する理由もない．

しかし，これらの考え方は，外部に対する説明責任という観点からは問題がある．計算機が適切に管理されていることを示すために，台帳を管理し，いつでも開示できることが必要である．また，管理台帳の維持は，説明責任を果たすという目的のみならず，固有網における計算機運用の方針を検討する際のよい資料となることは言うまでもない．

そこで，本稿では，管理台帳への登録を個々の利用

† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†† 岡山大学工学部
Faculty of Engineering, Okayama University

者自身に委ね，利用者自身が管理台帳を更新するように誘導するための仕組みを提案する．具体的には，利用する計算機の台帳登録や更新状況に応じて利用者の計算機を3つのクラスに分ける．そして，クラスに応じたIPアドレスをDHCPサーバによって付与する．固有網に設置されたWebサーバやメールサーバは，旧来のIPアドレスベースの利用制限をすることで，管理の容易さを維持したまま管理台帳維持を促進する．

以降，第2章では，想定する固有網環境と解決すべき課題について述べる．第3章では，課題を解決するための手法について提案する．第4章では，提案手法の実装と評価について述べ，最後に第5章で本稿をまとめる．

2. 想定環境と課題

2.1 想定環境

本稿で想定する固有網環境は，数十台の計算機を数部屋に分散配置し，一部あるいは大部分のIPアドレスをDHCPサーバで動的設定している環境である．具体的には，以下の機器やソフトウェアから構成されている．

(1) 管理対象計算機
数部屋に分散配置された30〜70台程度の計算機で，通常，1人の利用責任者が占有し長期に渡って使用する．ネットワークスイッチを介して相互に接続されている．各部屋の末端のスイッチは，安価なスイッチングハブである．

(2) ゲートウェイ (ファイアウォール)
外部のネットワークと接続するルータ機器である．ファイアウォール機能やNAT機能によってプライベートアドレスによる運用をすることも多い．

(3) DHCPサーバ
管理対象計算機にIPアドレスを動的に付与するためのサーバである．これによってIPアドレス管理の負担を軽減している．

(4) 各種ネットワークサーバ
利用者サービスのためのサーバ計算機とソフトウェアである．Webサーバ，メールサーバなどがこれに該当する．

(5) 計算機管理台帳 (CMDB)
全ての管理対象計算機について，利用責任者，設置部屋，使用IPアドレス，MACアドレス，導入済ソフトウェア一覧を記録したデータベースである．以下，CMDBと略記する．電子化され，Webブラウザ系由で管理することができるものとする．これは，専任の計算機管理者が維持更新する場合と，管理者の求めに応じて各利用責任者が更新する場合が考えられる．

2.2 課題

上記の想定環境において，利用者と管理者の負担を最小限にしつつCMDBを維持更新したい．具体的には，以下の課題があげられる．

(1) 招かざる客にはアクセス制限を施したい
未知の計算機には，何らかのアクセス制限を施したい．

(2) 一時利用者に便宜を計りたい
来客の求めに応じてDHCPで一時的に利用可能なIPアドレスを提供したいことがある．この場合，CMDBへの登録を強いる必要はない．通常の利用者と何らかの区別が必要である．

(3) 利用責任者にCMDB入力を任せたい
常時利用の計算機について，利用責任者自らがCMDB入力をしてくれるように誘導したい．そのためには，何らかの強制力が必要である．例えば，CMDBに未登録の計算機には固有網利用に制限をかけるなどの方法が考えられる．

(4) CMDBの更新忘れを防ぎたい
利用責任者，設置部屋等の情報は，年度の変り目といった決まった時期に変更が発生することが多い，あるいは使用していない計算機のIPアドレス解放や廃棄された計算機の登録抹消を忘れがちである．これらを防ぐため，周期的な更新を促す仕組みが必要である．

(5) 割り当てるIPアドレスを固定化したい
CMDB登録済みの管理対象計算機に割り当てるIPアドレスは固定化しておくことで，CMDBの管理と障害発生時の対応を容易にしたい．

(6) 管理対象計算機の設定を最小限にしたい
IPアドレス固定化のための特別な設定を管理対象計算機の利用者に求めない．つまり，DHCPによるアドレス割り当て設定のままで，DHCPサーバ側でIPアドレス付与の固定化をしたい．

(7) ネットワーク機器を増やしたくない
各部屋のスイッチングハブを高機能な物に変更し，VLANを構成してCMDB登録済計算機と未登録計算機をゲートウェイで分離することも考えられる．いわゆる利用者認証ゲートウェイの考え方である．こうした公共スペースに設置された公開端末[1]やISPが提供するHotspotで利用される技術[2]によって要求を実現するこ

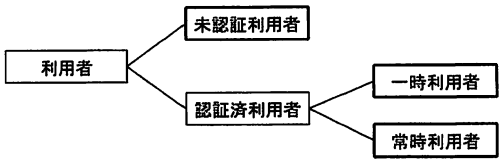

図 1　利用者クラス

表 1　利用者クラスとその特徴

利用者クラス	利用者の状態		固有網の利用権限	
	CMDB	認証	制限	期限
未認証利用者	未登録	未	有	無
一時利用者	未登録	済	無	短 (日)
常時利用者	既登録	済	無	長 (年)

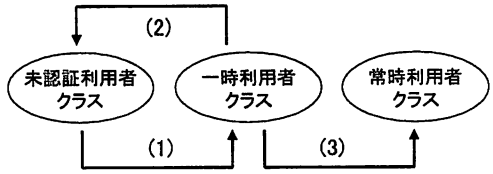

図 2　利用者クラス間の状態遷移図

とも考えられる．しかし，管理の手間やコストからこのような機器の導入は採用しづらい．

3. 利用者クラスを考慮した IP アドレス割り当て手法

3.1 利用者クラス

2.2 節で挙げた課題実現のためには，招かざる客，一時利用者，常時利用者の計算機を区別して，それぞれに応じた固有網に対する利用制限が必要である．そのためにまず，利用者クラスという概念を導入する．2.2 節の (1)〜(4) から導出される利用者クラスの分類を**図 1** に示し，以下に説明する．

(1)　未認証利用者クラス
認証を受けていない未知の利用者のクラスである．最初に固有網に接続した利用者の計算機は，全て未認証利用者クラスの計算機として扱われ，固有網の利用に制限がかけられる．

(2)　一時利用者クラス
信頼のおける利用者として認証を受けた利用者のクラスである．制限のない固有網の利用が可能であるが，比較的短い (1 日程度) 利用期限が付けられる．

(3)　常時利用者クラス
固有網を長期間にわたって利用する利用者のクラスである．このクラスの計算機は，CMDB に登録済みで，制限のない固有網を長期に渡って利用できる．しかし，あまり長期の利用期間を与えると，CMDB の登録情報が古いまま更新されない可能性があるので，1 年程度の利用期限を設定することが望ましい．

これらの比較を**表 1** に示す．表 1 は，利用者の認証と CMDB 登録状態に応じた固有網の利用権限を規定している．

3.2 利用者クラス間の状態遷移

次に，利用者クラス間の状態遷移規則を規定し**図 2** に示して以下に説明する．

(1)　未認証利用者クラスから一時利用者クラス
未認証利用者クラスの利用者は，制限付きの固有網接続を利用して，認証用の Web ページにアクセスし，そのページで管理者が事前に通知したパスワードを入力する．これによって，認証が得られて状態遷移が起こる．

(2)　一時利用者クラスから未認証利用者クラス
一時利用者クラスで一定の期間 (1 日程度) が経過すると無条件に状態遷移が起こる．

(3)　一時利用者クラスから常時利用者クラス
一時利用者クラスの利用者が，CMDB に計算機情報を入力することで，状態遷移が起こる．

(4)　常時利用者クラスから未認証利用者クラス
一時利用者クラスで一定の期間 (1 年程度) が経過すると無条件に状態遷移が起こる．

この状態遷移規則に従うことで，表 1 で示した利用者の状態と一致させることができる．

3.3 利用者クラスの識別

固有網の利用制限と期限を定めるために，個々の計算機の利用者クラスを識別する必要がある．この識別結果は，Web サーバや DNS へのアクセス制限，DHCP サーバのリース時間の決定などに利用される．識別には，表 1 で示した利用者の状態を知ることで識別可能であるであるが，Web サーバ，DNS，DHCP サーバ等の個々のサーバ全てが，認証結果や CMDB への登録状況を知るようにすることは難しい．

そこで，DHCP サーバのみが利用者の状態から利用者クラスを決定し，割当てる IP アドレスを利用者クラスに応じて変更する．これによって利用者クラスは IP アドレスによって識別可能になるので，各種サーバが旧来から備えている IP アドレスベースのアクセス制限が利用できる．

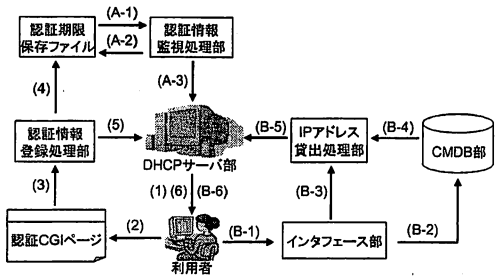

図 3　動作概要

3.3.1 IP アドレス切替えにかかる時間

前節で述べたように，各利用者クラス間の遷移に伴って，IP アドレスの付け替えが発生しうることになる．その切替えに要する時間について述べる．

IP アドレス切替えに要する時間は，DHCP サーバがクライアントに IP アドレスを与える際に通知するリース期限によって変化する．DHCP クライアントの OS が Windows の場合，リース期限の 50%が経過すると，DHCP サーバに IP アドレス更新依頼のパケットを送出する．この時点で，状態遷移が起こっていると，IP アドレス切替えが起こる．すなわち，IP アドレスが切替わるまでの時間は，最大でリース期限の 50%となる．

そこで，リース時間を短く設定することで，IP アドレス切替えまでの時間を短くすることが可能であるが，IP アドレス更新依頼のパケットの数が増大してしまい，固有網上に無駄なパケットが多く送信されてしまう可能性がある．

4. 実装と評価

4.1 実　　装

提案した利用者クラスを考慮した IP アドレス割り当て手法の有効性を確認するため，実装を行った．以下，実装内容と動作の概要について**図 3** に示して説明する．

4.1.1 実 装 内 容

DHCP サーバ部

フリーソフトウェアである ISC 版の DHCP[3] をそのまま使用した．

CMDB 部

CMDB 部は，計算機情報を管理するための RDBMS + Web CGI である．Ruby[4] とその Web フレームワーク Ruby on Rails[5] を利用した．

IP アドレス貸出処理部

IP アドレス貸し出し処理部は，DHCP サーバ部と CMDB 部を連携させるための処理部である．DHCP サーバ部の IP アドレス貸し出し状況を確認し，更新があれば CMDB 部を更新する．また，CMDB 部の計算機情報を DHCP サーバの設定ファイルに追加や更新する．

認証 CGI ページ

認証 CGI ページは，パスワード，ホスト名，MAC アドレスの入力フォームを設けた Web ページになっている．MAC アドレスについては，認証 CGI ページにアクセスした時点で，認証 CGI ページが自動的に取得し，入力フォームに補完する．認証が成功したら，認証情報登録処理部に，ホスト名と MAC アドレスを渡す．

認証情報登録処理部

認証情報登録処理部は，認証 CGI より取得したホスト名，MAC アドレス，そして現時刻から決定した認証期限を認証期限保存ファイルに書き出す．次に，認証を行った計算機に対し，制限のない IP アドレスを割り当てるように DHCP サーバの設定を動的に変更する．動的変更は，ISC 版 DHCP の Version 3 に標準搭載されている omshell を用いた．

認証期限保存ファイル

認証期限保存ファイルは，認証を行った計算機のホスト名，認証期限，MAC アドレスを保存している，テキスト形式のファイルである．

認証情報監視処理部

認証情報監視処理部は，認証期限保存ファイルを定期的に読み込み，認証期限が経過した計算機を探すデーモンである．認証期限が経過した計算機を発見した場合，認証期限保存ファイルから当該計算機の情報を削除する．また，制限のない IP アドレスを割り当てていた DHCP サーバの設定を omshell を利用して削除する．

4.1.2 動 作 概 要

(1) DHCP サーバ部は，固有網に接続してきた計算機に対し，動的に制限付 IP アドレスを割り当てる．

(2) 利用者は，制限付 IP アドレスを用いて，認証 CGI ページにアクセスし，利用する計算機のホスト名とパスワードを入力する．

(3) 認証 CGI ページは，利用者が入力したパスワードを照合する．パスワードが正しければ，認証を行った計算機のホスト名と，認証 CGI ページが自動で取得した IP アドレスから MAC ア

ドレスを求め，認証情報登録処理部に渡す．

(4) 認証情報登録処理部は，認証期限保存ファイルに認証を行った計算機のホスト名，認証期限，MACアドレスを追加する．

(5) 認証情報登録処理部は，DHCPサーバ部の設定に，認証を行った計算機に対して無制限IPアドレスを割り当てる設定を追加する．

(6) DHCPサーバ部は，認証を行った計算機に対し，動的に無制限IPアドレスを割り当てなおす．

ここで，処理が分岐する．計算機情報を登録する必要のない一時的な利用者は，以下の処理が行われ，認証期間が終了する．

(A-1) 認証情報監視処理部は，認証期限保存ファイルを定期的に読み込み，認証期限が経過した計算機を探す．

(A-2) 認証期限が経過した計算機を発見した場合，該当計算機の認証情報を削除する．

(A-3) 認証情報監視処理部は，DHCPサーバ部の設定で，認証期限を経過した計算機の無制限IPアドレスを割り当てる設定を削除する．

再び制限のない固有網の利用を行いたい場合は，(1)に戻り，再度認証を行う必要がある．そのため，計算機情報の登録をしないで，永続的に固有網を利用することは，認証が切れる度に再認証を行わければならないため，余計な負担が課せられる．

永続的に固有網を利用するには，計算機情報をCMDBに登録し，静的にIPアドレスを割り当てられなければならない．その場合の動作概要は(6)から以下の処理になる．

(B-1) 利用者は，無制限IPアドレスを用いて，インタフェース部にアクセスし，計算機情報を登録する．

(B-2) インタフェース部は，CMDBに計算機情報を追加する．

(B-3) インタフェース部は，IPアドレス貸出処理部に対してCMDBの更新を通知する．

(B-4) IPアドレス貸出処理部は，CMDBより計算機情報を取得する．

(B-5) IPアドレス貸出処理部は，DHCPサーバ部の設定に，計算機情報を登録した計算機に対して，無制限IPアドレスを静的に割り当てる設定を追加する．

(B-6) DHCPサーバ部は，計算機情報を登録した計算機に対し，静的に無制限IPアドレスを割り当てなおす．

4.2 評　　価

IPアドレス切替えにかかる時間について評価を行った．認証完了時に，無制限IPアドレスに切替わるまでに長時間を要してしまうと，利用者はIPアドレスが切替わるのを待たなければならなくなってしまい，利便性が低下する．そこで対処として，3.3.1節で述べた，DHCPサーバのリース時間短縮を行い，実際のIPアドレス切替え時間についての測定とリース時間短縮による計算機への影響の確認を行った．

IPアドレス切替えに要する時間は，DHCPサーバで設定するIPアドレスのリース時間に比例して変動する．そこで，IPアドレスのリース時間に様々な値を与え，実際にIPアドレスが切替わるまでに要した時間を測定を行った．

測定環境を**図2**に示し，測定結果として，切替わるまでの最長時間，最短時間，平均時間をまとめたものを**図4**に示す．

これらの結果から，リース時間を10秒程度と短い時間にすることで，利用者にIPアドレス切替えにかかる時間を3秒程度に抑えることができることが分かった．

この際，リース時間は，通常の運用にくらべて極端に短いが，利用者の計算機に影響は見られなかった．また，リース時間短縮化によるIPアドレス更新依頼のパケット数増大についても，影響は見られなかった．

表2 測定環境

クライアント台数	10台
クライアントOS	Windows XP Home Edition
回線環境	100Mbpsの Ethernet
測定方法	各クライアント機が任意のタイミングで認証を行い，クライアント機のIPアドレスが制限付IPアドレスから無制限IPアドレスに替わるまでの時間を測定．

5. おわりに

本稿では，DHCPサーバを用いた利用者管理システムを提案した．具体的には，利用者クラスに応じたIPアドレスを割り当てる手法について述べた．

想定する環境とそれに対する管理の課題を述べ，その対処として，利用者を分類し，各利用者の分類を利用者クラスとして定義を行い，その利用者クラスに応じて制限を行う手法を提案した．次に，提案手法についての設計方針を述べ，提案手法を実現する機構について，各クラスの仕様と各クラス間の状態遷移について述べた．さらに，DHCPサーバを利用し，IPアド

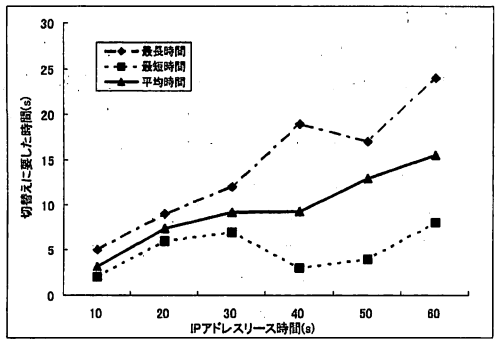

図 4　測定結果

レスの値そのものに制限情報を付加することで，固有網の利用を制限する手法について述べた．そして，提案手法を実現する機構の設計と動作概要について述べた．また，利用者クラスの変更にともなう IP アドレス切替えにかかる時間について検討した．最後に，実装と動作の概要について述べ，IP アドレス切替え時間の測定を行った．評価の結果，IP アドレス切替え時間は，DHCP サーバのリース時間を 10 秒程度と短い時間に設定することで，3 秒程度に抑えられることが分かった．

残された課題としては，固有網内の管理対象計算機同士の接続に対する制限がある．

参 考 文 献

1) 渡辺義明，渡辺健次，江藤博文，只木進一，“利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発”，情報処理学会論文誌,Vol.42, No.12, pp.2802-2809 (2001.12)
2) IEEE 802.1X, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf
3) ISC, “ISC-DHCP,” http://www.isc.org
4) Ruby, http://www.ruby-lang.org/
5) Ruby on Rails, http://www.rubyonrails.org/