特 別 研 究 報 告 書

題 目

DHCP と DNS を連携させる
計算機管理データベースシステムの実装と評価

提 出 者

岸 壮暁

岡山大学工学部 情報工学科

平成 21 年 2 月 6 日 提出

要約

現状の計算機情報の把握や，障害発生時の迅速な対処のために，計算機情報の管理が求められている．しかし，計算機情報の管理状況は組織によって様々である．例えば，DHCP サーバを介して計算機の接続を自由に許しているところもあれば，厳格な台帳管理を実施しているところもある．前者は，障害対応が困難になる以外に，外部への説明責任という観点からも問題がある．後者は，台帳の管理 (現状との同期など) に労力を要する．また，教育機関では，専任の業務チームを置くことが難しく，利用者の大半は学生であるため，規律を徹底し辛い．

現状と台帳との同期の問題を解決すべく，計算機管理データベース (CMDB) と DHCP を連携させる手法が提案された．しかし，CMDB は固有網利用において重要となる DNS データベースとの同期が取れていない．また，完全な実装と実用環境でのテストも行われていない．そこで，本論文では，DHCP と DNS を連携させる新しい計算機管理データベースシステムを提案する．提案システムは，DNS データベースを自動で管理して CMDB と同期を取る．また，IP アドレスベースの利用制限をしつつ，利用者自身で CMDB を更新するように誘導する．この利用制限では，利用者の状態に応じて IP アドレスの切り替わりが起こる．IP アドレスの切り替わりに時間がかかると，利用者は円滑に固有網を利用できない．

評価では，上記の観点から，IP アドレスが切り替わるまでの時間の測定と，DNS キャッシュの影響について評価した．評価の結果，IP アドレスが切り替わるまでの時間は，DHCP サーバのリース時間を 10 秒から 20 秒程度と短い時間に設定することで，12 秒程度に抑えられることが分かった．DNS キャッシュの影響については，IP アドレスが切り替わるまでの時間が 12 秒程度だったことを考慮し，DNS サーバの TTL を 10 秒に設定してキャッシュの影響が無いことを確認した．

目次

図 目 次

表 目 次

第 1 章

はじめに

大学の研究室や企業の部署では比較的小規模な計算機ネットワーク (以下，固有網と呼ぶ) が構築されている．近年，計算機の導入が容易になったことにより，このような固有網に所属する計算機の台数は増加している．このため，現状の計算機情報の把握や，障害発生時の迅速な対処のためにも，計算機情報の管理が求められている．

しかし，計算機情報の管理状況は組織によって様々である．例えば，DHCP(Dynamic Host Configuration Protocol) を介して計算機の接続を自由に許しているところもあれば，厳格な台帳管理を実施しているところもある．前者は，障害対応が困難になる以外に，外部への説明責任という観点からも問題がある．後者は，台帳の管理 (現状との同期など) に労力を要する．また，教育機関では，専任の業務チームを置くことが難しく，利用者の大半は学生であるため，規律を徹底し辛い．

現状と台帳との同期の問題を解決すべく，計算機管理データベースと DHCP を連携させる手法が提案された [1][2]．しかし，計算機管理データベースは固有網利用において重要となる DNS(Domain Name System) データベースとの同期が取れていない．また，完全な実装と実用環境でのテストも行われていない．

そこで，本論文では，DHCP と DNS を連携させる計算機管理データベースシステムを提案する．提案システムは，DNS データベースを自動で管理して計算機管理データベースと同期を取る．また，IP アドレスベースの利用制限をしつつ，利用者自身で計算機管理データベースを更新するように誘導する．DNS 管理，データベース管理，ライセンス管理等の手間を削減し，自律的な管理を目指す．

第 2 章

計算機管理データベース

2.1　計算機情報

計算機管理データベース (以下，CMDB と呼ぶ) は，固有網内に所属する計算機情報を管理するためのデータベースである．ここで，計算機情報とは計算機の管理者やその設置場所といった計算機に関する情報のことである．具体的な計算機情報を以下に示す．

(1) 管理者名
(2) ホスト名
(3) コード番号
(4) OS
(5) CPU の種類
(6) CPU の周波数
(7) メモリ容量
(8) MAC アドレス
(9) IP アドレス
(10) 設置場所
(11) ソフトウェアライセンス
(12) 備考

これらの情報を管理することで，現状の計算機情報を把握し，障害発生時には迅速な対処が可能となる．

2.2 計算機管理データベースの現状

2.2.1 利用者クラス

計算機管理データベースの現状として，まず，利用者クラスという概念がある [1]．利用者クラスの導入により，固有網の安全性を確保できる．また，2.2.2 項で説明する利用者クラスの状態遷移により，利用者自身の手によって CMDB を管理することが可能となっている．利用者クラスによる利用者の分類を図 2.1 に示し，以下で説明する．

未認証利用者クラスでは，不正目的な利用者による不正行為を防止するため，固有網の利用に制限をかける．一時利用者クラスでは，制限の無い固有網の利用を可能にするが，利用期限を設ける．常時利用者クラスでは，制限の無い固有網の利用を，無期限で利用できる．

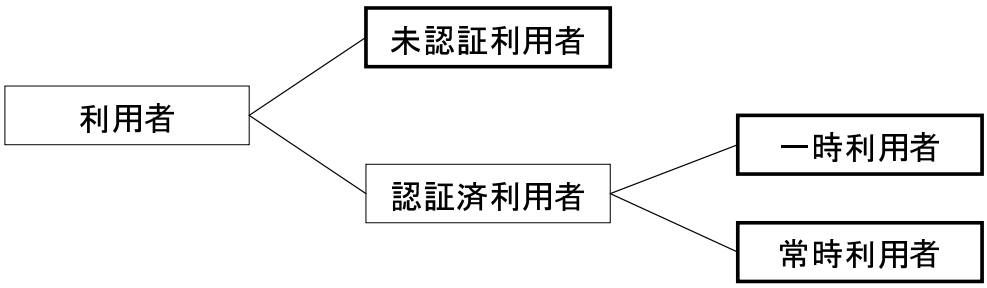

図 2.1 利用者の分類

利用者クラスの特徴を表 2.1 に示し，以下で詳細を述べる．

(1) 未認証利用者クラス
未認証利用者クラスとは，認証を受けていない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，動的に制限がかけられた IP アドレス (以下，制限付き IP アドレスと呼ぶ) を割り当てられる．

(2) 一時利用者クラス
一時利用者クラスとは，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．一時利用者クラスの計算機では，動的に制限がかけられていない IP アドレス (以下，無制限 IP アドレスと呼ぶ) を割り当てられ，制限のない固有網の利用を行うことができるが，比較的短い (1 日程度) 利用期限が設けられている．

(3) 常時利用者クラス
常時利用者クラスとは，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．常

時利用者クラスの計算機では，静的に無制限 IP アドレスが割り当てられ，制限のない固有網を永続的に利用することが可能である．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．

表 2.1 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)

2.2.2 CMDB を用いた自律管理

CMDB をシステム管理者がすべて管理するのは負担であるため，計算機情報の登録や更新は利用者に行ってもらいたい要求がある．そこで，利用者クラス間の状態遷移を利用する [2]．利用者クラス間の状態遷移を図 2.2 に示し，以下で説明する．

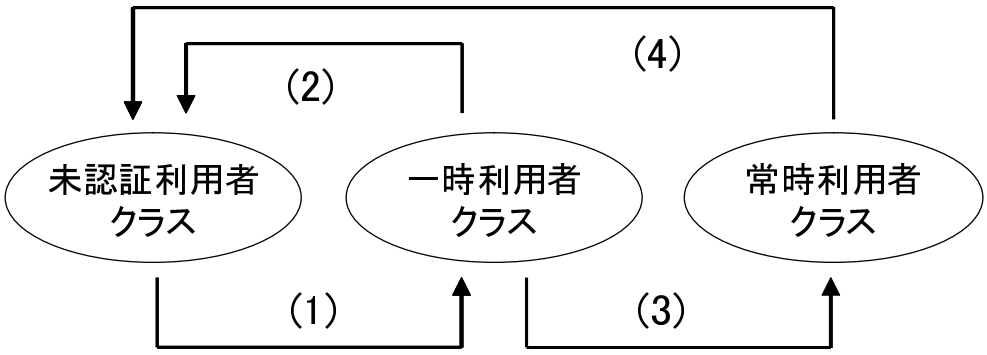

図 2.2 利用者クラス間の状態遷移

(1) 未認証利用者クラスから一時利用者クラスへの遷移

未認証利用者クラスから一時利用者クラスへの状態遷移は，未認証利用者クラスの利用者が，割り当てられた制限付き IP アドレスを用いて，認証用の Web ページへアク

セスし，そのページでシステム管理者が事前に通知したパスワードを入力することで，認証が受けられ，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への遷移
一時利用者クラスから未認証利用者クラスへの遷移は，一時利用者クラスで一定の期間 (1 日程度) が経過すると，無条件に遷移が起こる．そのため，永続的な固有網利用者は，常時利用者クラスに遷移しない限り，一定期間ごとに再認証を受ける必要がある．

(3) 一時利用者クラスから常時利用者クラスへの遷移
一時利用者クラスから常時利用者クラスへの遷移は，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への遷移
常時利用者クラスから未認証利用者への遷移は，常時利用者クラスで一定の期間 (1 年程度) が経過すると，無条件に遷移が起こる．

固有網の常時利用には，CMDB への計算機情報登録が必須になることを利用して，CMDB を利用者自身の手によって維持することが可能となっている．

2.2.3 DHCP との連携

固有網における IP アドレスは，DHCP サーバによって管理されている．また，未認証利用者クラスにかける固有網利用の制限について，IP アドレスに制限を付加する方法が採用されている．IP アドレスに制限を付加することにより，DHCP サーバの設定のみを行うことで，容易に固有網の利用制限をかけることができる．

DHCP サーバで計算機に IP アドレスを割り当てる際，DHCP サーバは割り当てる IP アドレスと共に様々な情報を付加して，割り当てを受ける計算機に送信している．表 2.2 に，IP アドレスの付随情報の一例を示す．

IP アドレスに制限を付加する手法として，表 2.2 にある，DNS サーバのアドレスおよびデフォルトゲートウェイのアドレスを制限用の情報にすることで制限を実現している．

デフォルトゲートウェイのアドレスに制限用のアドレスを指定することで，この情報が付随している IP アドレスを割り当てられた計算機は，デフォルトゲートウェイの正しい IP アドレスを得ることが不可能になるため，デフォルトゲートウェイを利用不可能となる．このことから，固有網外ネットワークへの経路が不明となるため，固有網外ネットワークへの接続は不可能となる．

表 2.2 IP アドレスの付随情報例

項目名	詳細
IP アドレス	割り当てる IP アドレス
リース時間	IP アドレス割り当ての期限
ドメイン名	所属するドメイン名
DNS サーバ	DNS サーバのアドレス
デフォルトゲートウェイ	デフォルトゲートウェイのアドレス

同様に，DNS サーバのアドレスに制限用の IP アドレスを指定することで，その情報が付随している IP アドレスを割り当てられた計算機は，DNS サーバの正しいアドレスを指定することができず，DNS サーバの利用が不可能となる．

IP アドレスへの制限付加設定の例を表 2.3 に示す．

表 2.3 IP アドレスへの制限付加設定の例

	正規のアドレス	無制限アドレス	制限付アドレス
デフォルトゲートウェイ	192.168.1.1	192.168.1.1	192.168.100.1
DNS サーバ	192.168.1.10	192.168.1.10	192.168.100.10

一時利用者クラスの計算機は，正規の情報が付随している無制限 IP アドレスを DHCP サーバより割り当てられる．一時利用者クラスの計算機は，この情報を基に DNS サーバやデフォルトゲートウェイの正しい IP アドレスを得ることができ，これらを利用可能になる．

一方，未認証利用者クラスの計算機は，制限用の情報が付随してある制限付き IP アドレスを DHCP サーバより割り当てられる．未認証利用者クラスの計算機は，この情報からでは DNS サーバやデフォルトゲートウェイの正しい IP アドレスを得ることができず，これらの利用は不可能となる．

また，IP アドレスでアクセス制限を行っているその他のサービスから扱いやすい．

2.3 現状のシステム構成

2.3.1 システム構成

現状のシステム構成を図 2.3 に示し，以下に現状のシステムの各構成要素について説明する．

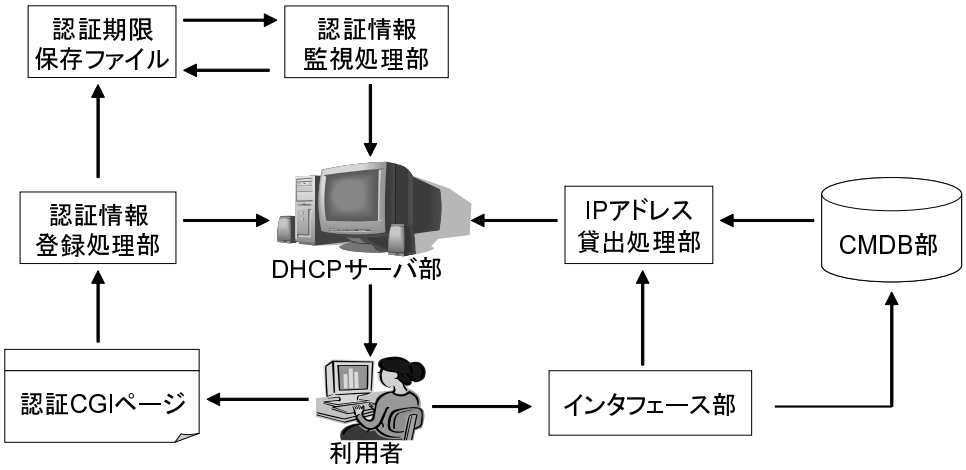

図 2.3 既存システムの構成図

(1) 認証 CGI ページ

認証 CGI(Common Gateway Interface) ページは，未認証利用者クラスの計算機が認証を受けるためのパスワード入力フォームを設定してある CGI ページである．

(2) 認証情報登録処理部

認証情報登録処理部は，認証を行った計算機のホスト名，MAC アドレスおよび認証期限を認証期限保存ファイルに書き出す．そして，その計算機に無制限 IP アドレスを割り当てるように，DHCP サーバの設定を変更する処理部である．

(3) 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，MAC アドレスおよび認証期限を保存しておくファイルである．

(4) 認証情報監視処理部

認証情報監視処理部は，定期的に認証期限保存ファイルを読み込み，認証期限が経過した計算機を見つけた際，認証期限保存ファイルより対象となる計算機の情報を削除する．そして，その計算機に制限付き IP アドレスを割り当てるように，DHCP サーバの設定を行う処理部である．

(5) DHCP サーバ部

DHCP サーバ部は，DHCP サーバの機能を提供する処理部である．

(6) インタフェース部

インタフェース部は利用者が計算機情報を登録する Web ページであり，計算機情報を CMDB に登録する処理部である．また，IP アドレス貸出処理部に対して CMDB の更新を通知する．

(7) CMDB 部
CMDB 部は，計算機管理データベースを用いた，計算機情報を管理するための処理部である．

(8) IP アドレス貸出処理部
IP アドレス貸出処理部は，DHCP サーバ部と CMDB 部を連携させるための処理部である．CMDB から情報を抽出し，無制限 IP アドレスを静的に割り当てる設定を DHCP サーバに追加する．

2.3.2 問題点

現状のシステム構成の問題点を以下に示す．

(1) 認証期限保存ファイル
認証期限保存ファイルには，認証を受けた計算機のホスト名，MAC アドレスおよび認証期限が記録されている．しかし，計算機のホスト名と MAC アドレスは計算機情報であり，本来は CMDB で管理されるべきである．

(2) IP アドレスの管理
現状のシステムでは，DHCP サーバの設定を認証情報登録処理部，認証情報監視処理部および IP アドレス貸出処理部が行っている．また，利用者に割り当てる IP アドレスを，制限付き IP アドレスは DHCP サーバ部が，動的無制限 IP アドレスは認証情報登録処理部が，静的無制限 IP アドレスは IP アドレス貸出処理部がそれぞれ管理している．IP アドレスの管理が複数箇所に分散しているのは，割り当てる IP アドレスの範囲を変更する場合などにシステム管理者の負担となり問題となる．

2.4 DNS データベース

DNS データベースは，計算機のホスト名と IP アドレスの対応を管理しており，計算機のホスト名から IP アドレスを，また，計算機の IP アドレスからホスト名を検索する機能を持

つ (それぞれ，正引き，逆引きと呼ぶ)．DNS データベースは，固有網内における各種サーバへのアクセスや電子メールの利用において必須となっており，厳格な管理が求められる．DNS データベースは CMDB とは別管理されており，現状では，CMDB に計算機情報が登録された後，システム管理者が手動で DNS の設定を行う．

2.5 課題

現状の計算機管理データベースシステムは，利用者クラスという概念を導入し，不正目的な利用者への対処と CMDB への計算機情報登録の促進を行っている．IP アドレスは DHCP サーバとの連携により管理され，また，IP アドレスには制限を付加する．これにより，DHCP サーバの設定のみを行うことで，固有網の利用に制限をかけることができる．しかし，DNS データベースは CMDB とは別管理されている．このため，CMDB に計算機情報が登録された後，システム管理者が手動で DNS の設定を行う必要があることから，DNS データベースと CMDB の同期は取れていない問題がある．

第 3 章

DHCP と DNS を連携させる 計算機管理データベースシステム

3.1　システムに対する要求

2.5 節で挙げた課題より，現状の計算機管理データベースシステムには以下の要求がある．

(1) DNS データベースの自動管理
システム管理者が手動で行っている DNS の設定を，システムが自動で設定できるようにする．

(2) CMDB と DNS データベースの同期
システム管理者が DNS データベースの設定を行っている状態では，CMDB と同期しているとは言えない．厳格に同期させようとすると，システム管理者の負担は増大する．このため，DNS データベースを自動管理しつつ，CMDB と同期させる．

3.2　提案システム

3.1 節で述べた要求を満たすシステムとして，DHCP と DNS を連携させる計算機管理データベースシステムを提案する．提案システムには，以下の特徴を持たせる．

(1) DNS データベースの自動管理
システム管理者が手動で行っている DNS の設定を，システムが自動で設定を行うよ

うにする．DNS の設定とは，具体的には計算機のホスト名から IP アドレスを，また，計算機の IP アドレスからホスト名を検索できるようにすることである．例えば，固有網のネットワークアドレスは 192.168.8.0/24，固有網のドメイン名は example.com の場合，ホスト名が host-PC，IP アドレスが 192.168.8.100 の計算機の対応付けを設定するには，DNS の正引き，逆引きのゾーンデータファイルにそれぞれ以下のように記述する．

```
host-PC IN A 192.168.8.100
100 IN PTR host-PC.example.com
```

DNS の設定を行うには，計算機のホスト名と IP アドレスが必要であり，計算機のホスト名と IP アドレスは CMDB で管理されている．従って，CMDB から計算機のホスト名と IP アドレスを取得し，システムが自動で DNS に設定を行うようにすればよい．

(2) CMDB と DNS データベースの同期

(1) では，DNS データベースを自動管理するために，CMDB から計算機のホスト名と IP アドレスを取得し，システムが自動で DNS の設定を行う方法について述べた．この方法を用いつつ，CMDB と DNS データベースの同期を取るためには，CMDB に計算機情報が新規に追加されたり，計算機情報の変更や削除が行われたりするたびに，DNS の設定を行う必要がある．つまり，CMDB の更新を契機として DNS の設定を行うことにより，最短時間で同期が取れるようになる．

第 4 章

システム設計

4.1 一時利用認証と常時利用認証

未認証利用者クラスから一時利用者クラスに遷移するために，認証用の Web ページへアクセスして行う認証を一時利用認証と呼ぶ．また，一時利用者クラスから常時利用者クラスに遷移するために，計算機情報登録ページへアクセスし，計算機情報を登録することを常時利用認証と呼ぶ．

4.2 現状のシステム構成の見直し

現状のシステム構成の見直しを行う．具体的には，2.3.2 項で挙げた認証期限保存ファイルと IP アドレスの管理の対処を行う．

4.2.1 認証期限保存ファイル

2.3.2 項で，計算機のホスト名と MAC アドレスは計算機情報であり，本来は CMDB で管理されるべきであることを述べた．また，CMDB に登録される計算機情報にも利用期限を設けることで，CMDB の更新忘れを防ぐ手法が提案されている [2]．つまり，CMDB で利用期限を管理することで，認証期限保存ファイルで管理されていた一時利用者クラスの計算機のホスト名，MAC アドレスおよび認証期限を常時利用計算機と同じように CMDB で管理できる．

一時利用認証を受けた計算機に無制限 IP アドレスを割り当てる処理は，CMDB から情報を取得し，DHCP の設定を行うことで実現する．以上の変更について図 4.1 に示し，以下で詳細を述べる．

一時利用認証を受けた計算機のホスト名，MAC アドレスおよび認証期限は，認証期限保存ファイルではなく CMDB に登録される．一時利用認証を受けた計算機に無制限 IP アドレスを割り当てる処理は，認証情報登録処理部が行っていたが，新たに設定適用処理部を設け，設定適用処理部が CMDB から情報を取得し，DHCP に割り当て設定を行う．

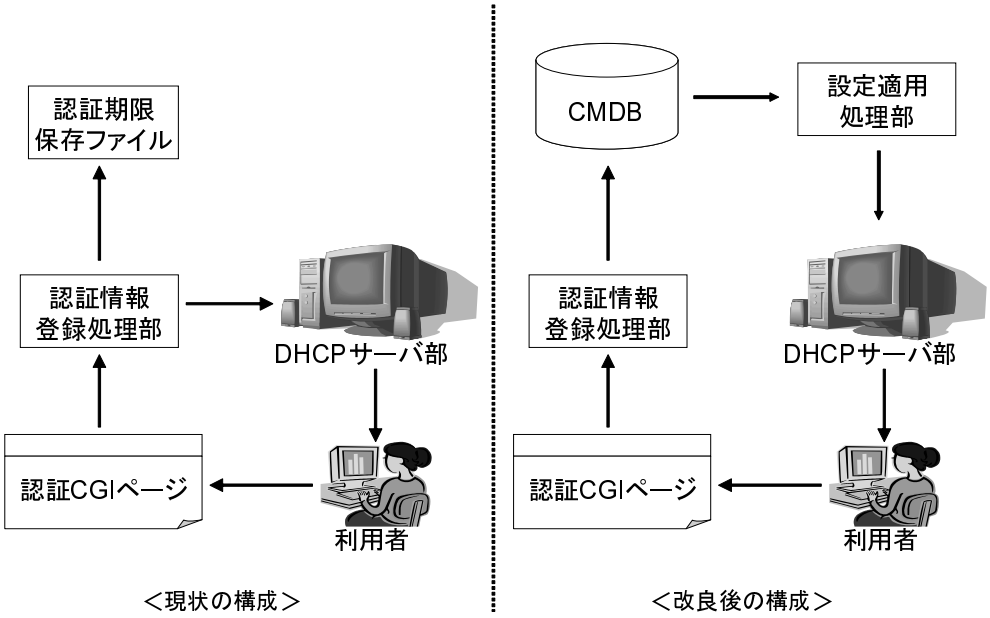

図 4.1 認証期限保存ファイルの内容を CMDB に統合

4.2.2 認証情報監視処理部

4.2.1 項で，認証期限保存ファイルを CMDB に統合した．これに伴い，認証情報監視処理部の動作を変更する．変更後の構成を図 4.2 に示し，以下で詳細を述べる．

認証情報監視処理部は，定期的に認証期限保存ファイルを読み込み，認証期限の経過した計算機を発見した場合，DHCP サーバに無制限 IP アドレスの割り当てを削除する処理を行っていた．この処理を以下のように変更する．

まず，認証情報監視処理部は，定期的に CMDB を読み込み，認証期限が経過した計算機情報を探す．認証期限が経過した計算機情報を発見した場合，その計算機情報を認証期限切

れに設定する．その後，設定適用処理部が CMDB から情報を取得し，無制限 IP アドレスの割り当てを設定しなおす．

さらに，認証情報監視処理部は，CMDB に登録されている常時利用者クラスの計算機情報についても利用期限が経過していないかを調査する．利用期限が経過した計算機情報を発見した場合，その計算機情報を利用期限切れに設定する．利用期限が切れた利用者は未認証利用者クラスとなり，再び一時利用認証，常時利用認証を受ける必要がある．これにより，CMDB は定期的に更新され，CMDB の情報が古いまま放置されるという状況を防止できる．

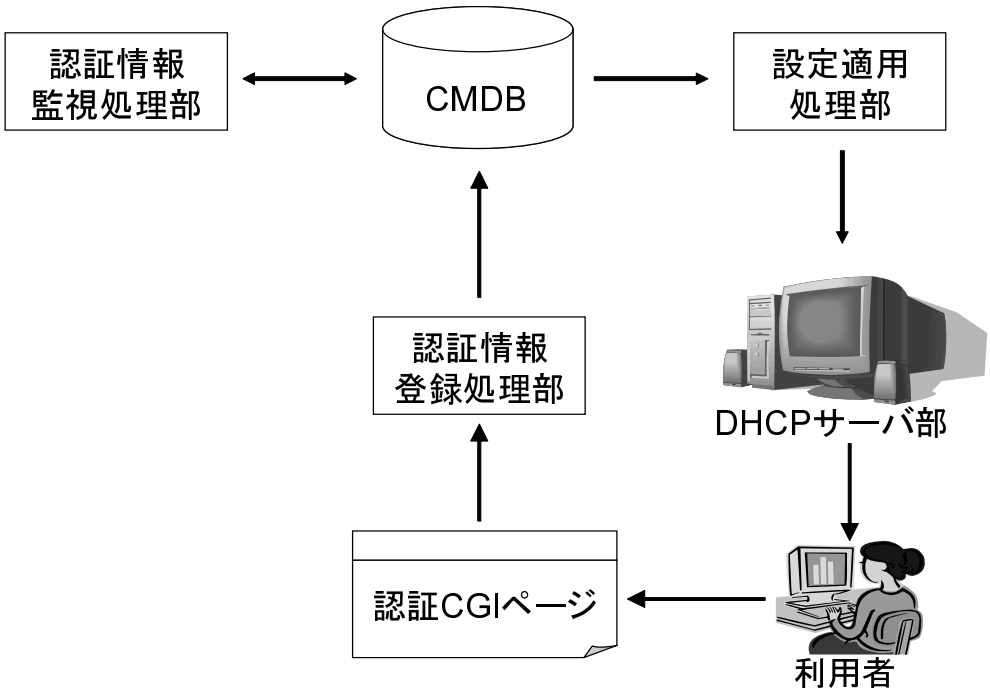

図 4.2 認証情報監視処理部の動作変更

4.2.3 IP アドレス貸出処理部

IP アドレス貸出処理部は，インタフェース部からの更新通知を契機として，CMDB から情報を抽出し，無制限 IP アドレスを割り当てる設定を DHCP サーバに追加する処理部である．これは，設定適用処理部と同じ処理を行うため，設定適用処理部に統合する．

4.2.4 DNS の設定

3 章で，DNS の自動管理について述べた．DNS の設定は，CMDB から情報を取得し，システムが自動で DNS の設定を行う．CMDB から情報を取得し，設定を行うという処理は，4.2.1 項，4.2.2 項で述べた設定適用処理部と同じ処理である．そのため，設定適用処理部は，CMDB から情報を取得し，DHCP の設定と DNS の設定を行う処理部とする．また，CMDB と DHCP，DNS の同期を取るため，設定適用処理部は CMDB の更新を契機として，DHCP と DNS の設定を行う．このため，設定適用処理部はインタフェース部から CMDB の更新通知を受け取る必要は無くなる．

4.2.5 IP アドレスの管理

現状のシステム構成では，DHCP サーバの設定を認証情報登録処理部，認証情報監視処理部および IP アドレス貸出処理部が行っている．システム構成の見直しを行った結果，DHCP の設定を行うのは設定適用処理部のみとなった．IP アドレスの管理が分散されること無く，また，DHCP の設定は CMDB からのみ設定されるようになった．

4.3 DHCP と DNS の連携による利用制限

現状では，DHCP サーバを用いた利用制限を行っている．提案システムでは，DHCP と DNS の連携による利用制限を提案する．未認証利用者クラスの利用者には制限付き IP アドレスが DHCP サーバより割り当てられる．IP アドレスに制限を付加する手法として，DNS サーバのアドレスおよびデフォルトゲートウェイのアドレスを制限用の情報にすることで制限を実現している．提案システムでは，デフォルトゲートウェイのアドレスは制限用の情報にするが，DNS サーバのアドレスではこれを行わない．しかし，DNS サーバは，制限付き IP アドレスを持つ計算機からの問い合わせには，必ず認証ページを持つ計算機のアドレスを返すようにする．これにより，未認証利用者クラスの利用者には固有網の利用制限をかけつつ，認証ページへ誘導することが可能となる．

4.4 システム構成

4.2 節での変更をまとめた提案システムのシステム構成を図 4.3 に示す．以下では，システムの動作概要について説明する．

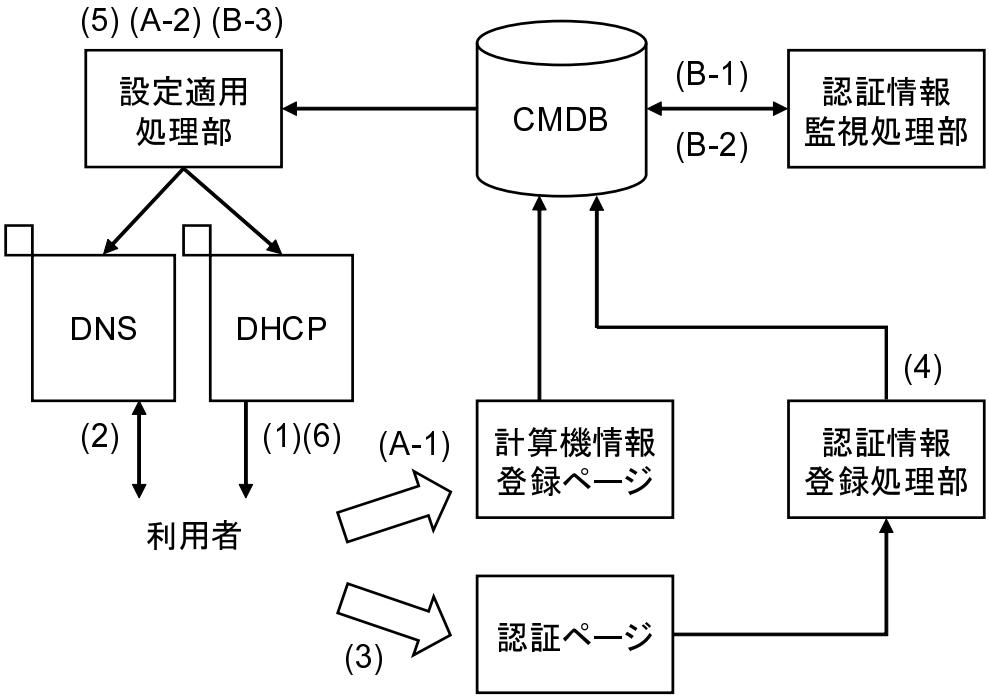

図 4.3 システム構成図

4.4.1 一時利用認証

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

(2) DNS サーバは，制限付き IP アドレスからの問い合わせには必ず認証ページの IP アドレスを返す．これによって，利用者を認証ページへ誘導する．

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

(4) 認証情報登録処理部は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，MAC アドレス，認証期限，新たに割り当てる無制限 IP アドレスを CMDB に登録する．

(5) 設定適用処理部は CMDB から情報を取得し，DHCP と DNS の設定を行う．

(6) DHCP サーバは認証を行った計算機に対し，無制限 IP アドレスを割り当てる．

4.4.2 常時利用認証

(A-1) 利用者は，無制限 IP アドレスを用いて計算機情報登録ページへアクセスし，計算機情報を登録する．

(A-2) 設定適用処理部は CMDB から情報を取得し，DHCP と DNS の設定を行う．

4.4.3 認証期限

(B-1) 認証情報監視処理部は，CMDB を定期的に参照し，認証期限が経過した計算機情報を探す．

(B-2) 認証情報監視処理部は，認証期限が経過した計算機情報を発見した場合，その計算機情報を認証期限切れに設定する．

(B-3) 設定適用処理部は CMDB から情報を取得し，DHCP と DNS の設定を行う．

第 5 章

実装

5.1 実装内容

提案した DHCP と DNS を連携させる計算機管理データベースシステムの有効性を確かめるため，図 4.3 のシステムを 1 台の計算機上に実装した．実装内容を以下に示し，説明する．

(1) DHCP サーバ
フリーソフトウェアである ISC 版の DHCP[3] をそのまま使用する．

(2) DNS サーバ
フリーソフトウェアである BIND[4] を使用する．

(3) CMDB
CMDB は，計算機情報を管理するための RDBMS + Web CGI である．CMDB は，CMDB 内の情報が新規追加や削除などにより更新されると，設定適用処理部に DHCP と DNS の設定更新を通知する．CMDB の実装には Ruby[5] と Ruby on Rails[6] を利用した．

(4) 認証ページ
認証ページは，パスワードと計算機のホスト名の入力フォームを設けた Web CGI ページになっている．また，アクセス元の計算機の MAC アドレスを自動的に取得する．

(5) 認証情報登録処理部
認証情報登録処理部は，パスワードを照合する．パスワードが正しければ，新たに割り当てる無制限 IP アドレスを選択し，現時刻から認証期限を決定する．そして，この

無制限 IP アドレスと認証期限を，認証ページより取得した計算機のホスト名と MAC アドレスとともに CMDB に登録する．

(6) 計算機情報登録ページ
計算機情報登録ページは計算機の管理者や設置場所といった計算機情報の入力フォームを設けた Web CGI ページになっている．

(7) 設定適用処理部
設定適用処理部は，CMDB から情報を取得し，DHCP と DNS の設定を行う．具体的には，DHCP の設定では，CMDB から計算機のホスト名，IP アドレスおよび MAC アドレスを取得し，固定 IP アドレスを割り当てる設定を行う．DNS の設定では，CMDB から計算機のホスト名と IP アドレスを取得し，名前解決の設定を行う．その後，設定を適用させるため，DHCP サーバと DNS サーバを再起動する．

(8) 認証情報監視処理部
認証情報監視処理部は，CMDB を定期的に参照し，認証期限が経過した計算機情報を探すデーモンである．認証期限が経過した計算機情報を発見した場合， その計算機情報を認証期限切れに設定する．

5.2 CMDB と DNS の連携手法

DNS の設定を行う方法として，設定ファイルを編集する他に，Dynamic DNS Update[7] (以下，DDNS と呼ぶ) を利用する方法がある．

DDNS とは，DNS レコードの動的な追加と削除をサポートする機能である．DHCP は DDNS を利用することにより，固有網に接続した計算機のホスト名と IP アドレスを動的に DNS に登録することができる．また，固有網から接続を断った計算機のホスト名と IP アドレスを動的に DNS から削除することもできる．DHCP サーバがクライアントにどのような IP アドレスを割り当てたとしても，各サーバのアクセスログにはホスト名が記録される．また，割り当てられた IP アドレスが動的に変わっても，ホスト名で固定的にアクセスや識別ができるなどのメリットがある．

しかし，提案システムにおいて DDNS を用いた場合，DNS の設定を行うのは DHCP である．CMDB と DNS は別管理されていることになり，CMDB と DNS が同期しているとは言えない．これは，3 章で述べた要求を満足しない．

以上のことから，本実装においては，DNS の設定ファイルを直接編集する手法を採用した．

5.3 CMDB と DHCP の連携手法

認証済の利用者に割り当てられる IP アドレスは，CMDB 内の情報により決定される．DHCP サーバへの設定適用方法として，DHCP の設定ファイルを編集し，無制限 IP アドレスとして固定 IP アドレスを割り当てる設定を記述する手法，および omshell の利用がある．

ISC DHCP3 には，DHCP サーバの動的設定を行うための OMAPI という機構が組み込まれている．この機構をコマンドラインから扱うための shell が omshell である．omshell は OMAPI を通して DHCP サーバへ接続，DHCP サーバの状態を検査し，対話的に設定変更を行える．この際，DHCP サーバの停止，再起動は必要ない．また，omshell では，DHCP クライアントを操作することもできる．この操作では，DHCP クライアントの現在割り当てられている IP アドレスの解放や即座の再割り当てを行うことができる．

DHCP サーバの設定ファイルを直接編集する方法は，DHCP サーバと提案システムが同一計算機上にある場合，導入は容易であるものの，そうでない場合，実現は困難である．また，設定ファイル編集後，DHCP サーバの再起動が必要となり，システムに与える負荷は大きい．しかし，omshell は導入が難しい．また，omshell は一般に広く利用されているとは言い難く，実用例や利用法に関する文書が整備されていない．このため，omshell を利用する手法は，実装工数が大きくなる問題がある．ここで，提案システムを 1 台の計算機上に構築することから，実装の容易な DHCP サーバの設定ファイルを直接編集する手法を採用した．

第 6 章

評価

6.1　評価内容

6.1.1　IP アドレスが切り替わるまでの時間

未認証利用者クラスの利用者には，制限付き IP アドレスが割り当てられ，一時利用認証を受けると無制限 IP アドレスが割り当てられる．この IP アドレスの切り替わりに時間がかかると，円滑な固有網利用ができない．

一方，IP アドレスが切り替わるまでに要する時間は，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時間によって変化する．DHCP クライアントの OS が Windows の場合，リース時間の 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，利用者クラスの状態遷移が起こっていると，IP アドレスの切り替わりが起こる．また，本実装において，無制限 IP アドレスの割り当てには，DHCP サーバの設定ファイルに固定 IP アドレスを割り当てる設定を記述する手法を採用している．この設定を適用するには，設定ファイルを編集した後に DHCP サーバを再起動する必要がある．以上のことから，IP アドレスが切り替わるまでの時間は，最大でリース時間の 50%と DHCP サーバを再起動する時間の和になる．

このことから，リース時間を短く設定することで，IP アドレスが切り替わるまでの時間を短くすることが可能である．しかし，IP アドレス更新依頼のパケット数が増大してしまい，固有網に負荷がかかる可能性がある．このため，リース時間を変えることで，IP アドレスが切り替わるまでの時間はどのように変化するか測定し，同時に，固有網にかかる負荷について評価する．

6.1.2 DNS キャッシュの影響

Unix や Linux では，DNS サーバへの問い合わせ結果をローカルにキャッシュしない．

一方，Windows には DNS Client というサービスがあり，ローカルに DNS レコードをキャッシュしている．提案システムにおけるキャッシュの影響を以下に示し，説明する．

(1) 認証ページ
提案システムにおいて，未認証利用者クラスの利用者は，どこの URL へアクセスしようとしても認証ページへ誘導される．例えば，`http://www.example.com/`へアクセスしても認証ページが表示される．このとき，利用者の計算機にこの対応付けがキャッシュされる．利用者が一時利用認証を受けると，自由にネットワークを利用可能になる．しかし，再び `http://www.example.com/`へアクセスした場合，キャッシュの内容が参照され，認証ページが表示されてしまう．

(2) CMDB の更新
あるサーバ計算機 S が CMDB に登録されており，クライアント計算機 C がこのサーバ計算機 S にアクセスする．このとき，クライアント計算機 C にはキャッシュが残る．その後，サーバ計算機 S のホスト名や IP アドレスが変更され，CMDB の更新が行われる．クライアント計算機 C は，キャッシュの内容を参照し，サーバ計算機 S へアクセスを行おうとするが，キャッシュの情報は古いままなので，サーバ計算機 S にはアクセス不可能となる．

これらの DNS キャッシュの影響について評価する．

また，DNS サーバからの否定応答 (指定されたレコードは「存在しない」という結果が戻ってくる) が戻ってきた場合も，その結果はキャッシュされる．これをネガティブキャッシュと呼ぶ．ネガティブキャッシュが提案システムに影響を与えることはないため，ネガティブキャッシュの影響については評価を行わない．

6.2 評価結果

6.2.1 IP アドレスが切り替わるまでの時間

IP アドレスが切り替わるまでの時間は，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 アドレスが切り替わるまでに要した時間を測定した．

測定環境を表 6.1 に示し，測定結果として，切り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 6.1 に示す．

これらの結果から，リース時間を 10 秒から 20 秒程度の短い時間に設定することで，IP アドレスが切り替わるまでの時間を 12 秒程度に抑えられることが分かった．

この際，リース時間は，通常の運営に比べて極端に短いが，利用者の計算機に影響は見られなかった．

表　6.1　測定環境

クライアント台数	8 台
クライアント機の OS	Windows XP Home Edition，Windows Vista Business
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 アドレスが制限付き IP アドレスから， 無制限 IP アドレスに切り替わるまでの時間を測定した．

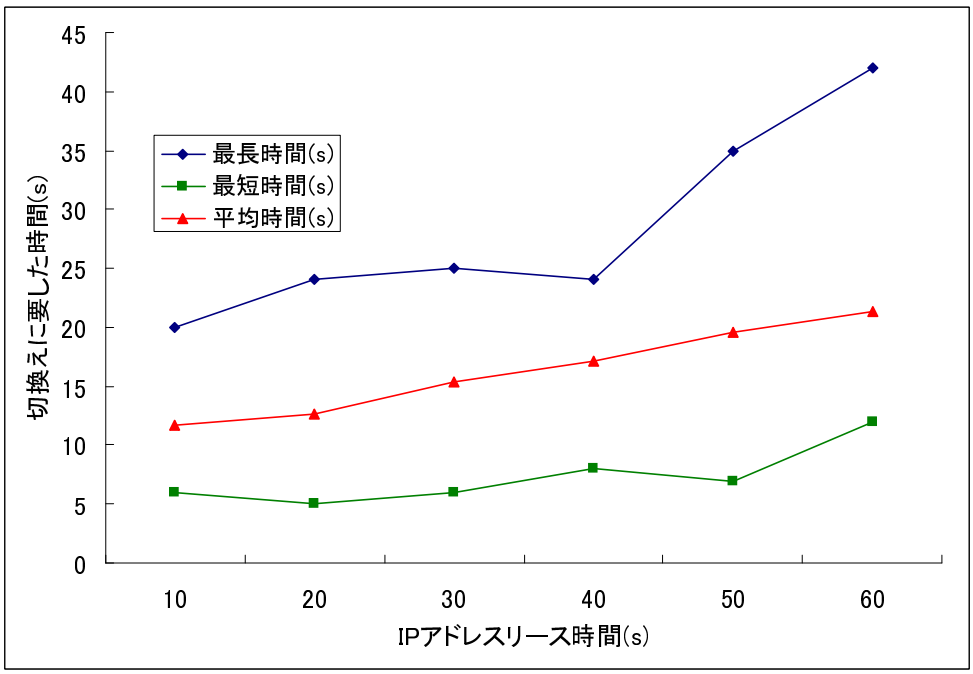

図　6.1　測定結果

6.2.2 DNS キャッシュの影響

Windows の DNS Client キャッシュに保持される時間には上限がある．DNS サーバから返された結果のレコードには必ず TTL(Time To Live，生存時間) が指定されている．TTL を超過した場合，キャッシュから破棄される．つまり，DNS サーバの TTL を適切な値に設定することで，6.1.2 項で述べた DNS キャッシュの影響を抑制できる．

(1) 認証ページ

6.2.1 項において，リース時間を 10 秒から 20 秒程度にすることで，IP アドレスが切り替わるまでの時間を 12 秒程度に抑えられることが分かった．このことから，DNS サーバの TTL を 10 秒以下に設定することで，IP アドレスが切り替わるのを待っている間にキャッシュが破棄されるようになると考えられる．

実際に，DNS サーバの TTL を 10 秒に設定した状態で一時利用認証を受け，その後のネットワーク利用で特に影響が無いことを確認した．

(2) CMDB の更新

本提案システムの実装において，CMDB が更新され，DNS サーバに CMDB の内容が反映される処理にかかる時間は，設定ファイルを編集し，DNS サーバを再起動するまでの時間であるため，数秒程度であると考えられる．そこで，DNS サーバの TTL を 10 秒に設定して動作確認を行い，特に影響が無いことを確認した．

第 7 章

おわりに

本論文では，DHCP と DNS を連携させる計算機管理データベースシステムについて述べた．

まず，計算機管理データベースと DHCP を連携させる手法について述べ，計算機情報，計算機管理データベースの現状，CMDB を用いた自律管理について述べた．次に，現状の計算機管理データベースシステムの課題として，DNS データベースをシステム管理者が手動で管理していること，CMDB と DNS の同期が取れていないことを述べた．

そこで，現状の計算機管理データベースシステムに対する要求を述べ，この要求を満たすシステムとして，DHCP と DNS を連携させる計算機管理データベースシステムを提案した．提案システムは，DNS データベースを自動で管理して CMDB と同期を取る．次に，現状のシステム構成の見直しを行った．そして，DHCP と DNS の連携による利用制限について述べた．さらに，提案システムのシステム構成を示し，動作概要について述べた．

次に，提案システムの実装内容について述べ，CMDB と DNS，DHCP の連携手法について述べた．

最後に，評価について述べ，IP アドレスが切り替わるまでの時間の測定と，DNS キャッシュの影響について調査した．評価の結果，IP アドレスが切り替わるまでの時間は，DHCP サーバのリース時間を 10 秒から 20 秒程度と短い時間に設定することで，12 秒程度に抑えられることが分かった．DNS キャッシュの影響については，IP アドレスが切り替わるまでの時間が 12 秒程度だったことを考慮し，DNS サーバの TTL を 10 秒に設定し，キャッシュの影響が無いことを確認した．

謝辞

本研究を進めるにあたり，懇切丁寧なご指導をしていただきました乃村能成准教授に心より感謝の意を表します．また，研究活動において，数々のご指導やご助言を与えていただいた谷口秀夫教授，田端利宏准教授に心から感謝申し上げます．

また，日頃の研究活動において，お世話になりました研究室の皆様に感謝いたします．

最後に，本研究を行うにあたり経済的，精神的な支えとなった家族に感謝いたします．

参考文献

[1] 入江 正博, “利用者クラスを考慮したIPアドレス自動割り当て手法,” 岡山大学工学部情報工学科卒業論文, 2006

[2] 乃村 能成, 入江 正博, 谷口 秀夫, “DHCPサーバを用いた利用者管理システムの提案,” 第127回DPS研究会 研究報告, pp.31-36 (2006.06).

[3] ISC, “ISC-DHCP,” https://www.isc.org/

[4] ISC, “ISC-BIND,” https://www.isc.org/

[5] David Flanagan, まつもと ゆきひろ, “プログラミング言語 Ruby,” オライリー・ジャパン (2009).

[6] Dave Thomas, David Heinemeier Hansson, “Agile Web Development with Rails,” The Pragmatic Bookshelf (2005).

[7] RFC2136, “DNS UPDATE,” http://www5d.biglobe.ne.jp/ stssk/rfc/rfc2136j.html

発表論文

[1] 岸 壮暁, 乃村 能成, “DHCP と DNS を連携させる計算機管理データベースシステム,” 電子情報通信学会 2009 年総合大会講演論文集, (掲載予定).