

IP アドレス管理用メンテナンスシステムの構築

若松 進*、鬼頭良彦*、千代谷一幸*

*工学研究科・工学部技術部 電子・情報技術系

はじめに

現在、工学研究科情報セキュリティ部会委員として「工学研究科 IP アドレス管理システム」等のメンテナンス業務を行っている。この IP アドレス管理システムは、ネットワークに接続されたパソコン等の端末情報を管理して、ネットワークトラブル発生時の早急な対応に利用されている。そのため、IP アドレスは、割当範囲内のアドレスを使用する必要があり、その割当設定は管理者が行う必要がある。

しかし、従来の割当設定は、手作業(直接データベースを操作)で行っているため、設定ミスを引き起こす可能性があった。そこで今回、この設定作業を Web アプリケーション化することにより、IP アドレス設定を正確に行う(ミスを回避できる)メンテナンスシステムを構築した。

1 . 目的と背景について

我々は、セキュリティ部会の実務担当者として、

- (1) 工学研究科の DNS(Domain Name System)の逆引きの設定
- (2) IP アドレス管理システムの運用
- (3) セキュリティ部会に関する情報の作成と公開

等を、我々が持っている技術を生かす形で得意分野について分担してきた。これらの管理作業の内、(1)と(2)については、迅速な対応が要求される。

そこで、これらの管理作業を円滑に行うため、本研修を行うに当たり、

- (1) 部会業務について、担当者間の技術レベル格差を少なくすること、
- (2) 今後の業務担当者の変更時に、管理業務の引継ぎが円滑に行われこと、

等を実現できる方法を検討することを目的とした。

具体的には、

- (1) 管理業務を正確、かつ迅速に行うため、複数担当者による管理体制の確立、
- (2) 部会業務の中から、緊急性の高い IP アドレス管理を優先して取り上げる、
- (3) その際、設定を確実にを行う方法を検討すること、
- (4) ソフトウェア開発は、初心者も含め全員で行うこと、
- (5) 開発には、言語 PHP を使用する

という方針で行うこととした。

このことにより、人的バックアップの確保、開発者の拡充、新しい言語への取り組みという、今後必要とされる業務実施方法についての検討も含めて行うことにした。

2 . IP アドレス管理について

名古屋大学では、大学全体の IP アドレス管理は、情報連携基盤センターが担当しており、各部局の規模に応じて IP アドレスが割当てられている。

一方、工学研究科の IP アドレス管理はセキュリティ部会が担当しており、各専攻は IP アドレスの希望割当範囲をセキュリティ部会に申請し、セキュリティ部会で審査・承認された後各専攻への IP 割当を行っている。そして、各専攻においては、それぞれの管理方針に従って研究室等への割当を行っている。

また、NICE に接続された各々の端末情報の管理については、各専攻の IP 管理者が「IP アドレス管理システム」を使用してデータベースに登録することによって実現している。

2.1. システムの概要

IP アドレス管理システムは、図 1. に示すように端末情報を Web 上から登録するプログラムと、関連したデータベースから構成されている。

このシステムでは、Web 画面上の入力項目の中の IP アドレスの設定値と、データベース（専攻情報、建物情報、割当範囲の各テーブル）の設定値との比較を行い、矛盾がない時には端末情報テーブルへの登録が行われ、その情報は同時に情報連携基盤センターのデータベースにも反映される。

このシステムでは、これら 3 つのテーブルが正しく設定されていることが前提となっている。

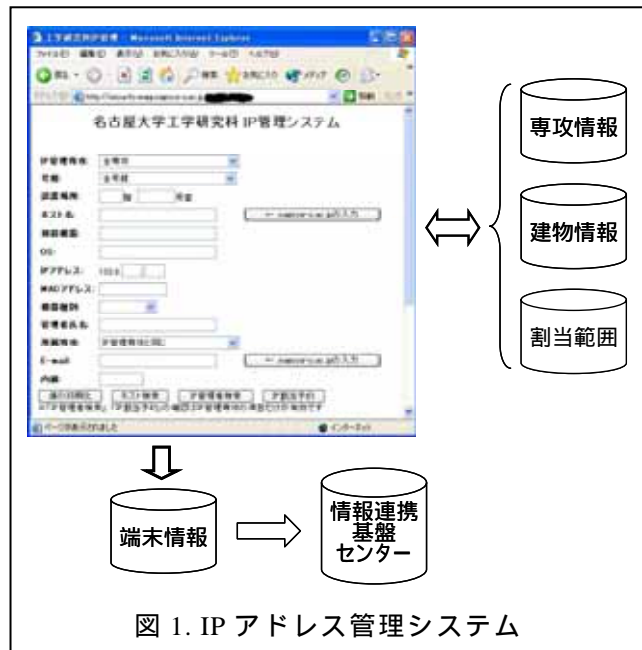


図 1. IP アドレス管理システム

2.2. 従来のテーブル設定法

図 1. に示した、データベース（専攻情報、建物情報、割当範囲の各テーブル）を設定するのに、従来の方法では、図 2. に示すように、直接データベースに接続して sql 文を実行することによって設定している。

この方法では、データベースの知識を必要とするだけでなく、sql 文の実行により無条件にデータベース操作が実行されてしまうので、データベース管理者は各専攻への「割当範囲」を設定する時に、その専攻に設定されている「専攻 ID」とその専攻の入居している「建物 ID」、及びその専攻に対する IP アドレス割当範囲のデータについての整合性を確認する必要がある。

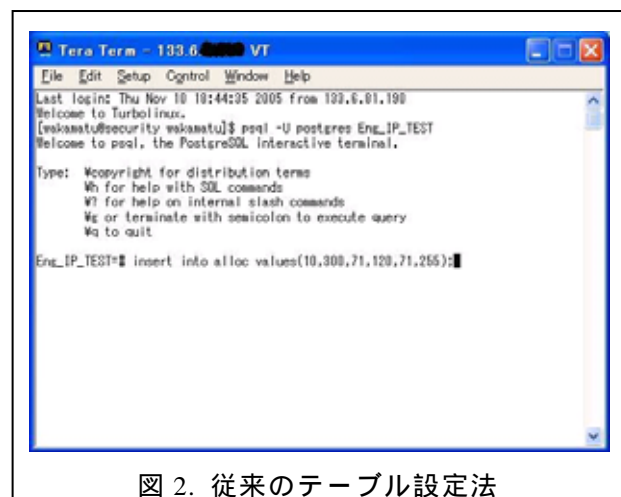


図 2. 従来のテーブル設定法

もし、この割当範囲の設定を間違えると、各専攻の IP アドレス管理者が、NICE に接続している端末情報を IP アドレス管理システムに登録する時、本来割当てられていない他専攻の割当範囲や他部局の割当範囲の使用が可能となるという状況が発生してしまう。その結果、IP アド

レス管理システムへの登録データは、情報連携基盤センターに誤った端末情報データを送ることにより、他部局の端末情報の書き換えという状況が発生して、他部局の IP アドレス管理に迷惑をかけることが起こってしまう。

3 . IP アドレス管理用メンテナンスシステム

工学研究科の IP アドレス管理をより確実に実行するためには、各専攻に対する IP アドレス範囲を簡単、かつ正しく設定するためのメンテナンスシステムの導入が必要である。このメンテナンスシステムの構築に当たり、従来から使用している IP アドレス管理システム、及びデータベースはそのまま使用する。

3.1. 使用するデータベース

IP アドレス管理システムの運用に必要なデータベースは、(1) 専攻の管理者情報 (Person)、(2) 管理者パスワード (Password)、(3) 専攻 IP 割当範囲 (Alloc)、(4) 専攻情報 (Dept)、(5) 建物情報 (Building)、(6) 端末情報 (Machine)、という 6 つのテーブルから構成されている。そして、メンテナンスシステムを構築するために、これら 6 つのテーブルに加えて、メンテナンスシステムの利用者を登録する (7) メンテナンス管理者用パスワード (Admin)、と工学研究科の IP 割当範囲を設定する (8) 工学研究科 IP 割当範囲 (Space) の 2 つのテーブルを追加した。

なお、メンテナンスシステムを利用するためには、Admin テーブルに登録されている必要がある。また、本システムにおいて、Web 上から設定することが出来るのは、従来直接データベースに接続して設定していた Alloc, Dept, Building の 3 つのテーブル、及び今回追加した Space テーブルの計 4 つのテーブル設定である。これらのテーブル情報について、表 1. ~ 表 4. に示す。

3.2. IP アドレスの割当チェック

IP 割当範囲に関するチェックが必要なのは、「専攻 IP 割当範囲」テーブルと「工学研究科 IP 割当範囲」テーブルの 2 つである。これら 2 つのテーブルの関係は、専攻 IP 割当範囲が常に工学研究科 IP 割当範囲内であるということである。

以下のこれらのテーブル設定時のチェック方法について記述する。

(a) 工学研究科 IP 割当範囲 (Space)

この割当範囲を設定する時、アドレス範囲の値については、情報連携基盤センターから割当てられた数値を指定しなければならない。そして、割当範囲について「追加登録」、「削除」、「範囲の変更」を行う時には、それぞれ次のチェックを行う。

追加登録：設定した IP アドレス範囲は登録データ (Space) との比較を行い、重複がなければ

表 1. 専攻 IP 割当範囲テーブル

項目名	項目変数	型
専攻番号	Deptid	Integer
号館番号	Buildid	Integer
開始第3	L3	Integer
開始第4	L4	Integer
終了第3	H3	Integer
終了第4	H4	Integer

表 2. 専攻情報テーブル

項目名	項目変数	型
専攻番号	Deptid	Integer
専攻名	Dept	Text

表 3. 建物情報テーブル

項目名	項目変数	型
号館番号	Buildid	Integer
号館名	Building	Integer

表 4. 工学研究科 IP 割当範囲

項目名	項目変数	型
開始 IP(3)	Ip_L3	Integer
開始 IP(4)	Ip_L4	Integer
終了 IP(3)	Ip_H3	Integer
終了 IP(4)	Ip_H4	Integer

その割当範囲は登録される。重複が確認された時、登録は拒否される。

削除：指定の割当範囲は専攻 IP 割当範囲 (Alloc) として登録されているデータとの比較を行い、その範囲内に専攻 IP 割当範囲が設定されていれば削除は拒否され、設定されていなければその割当範囲は削除される。

範囲の変更：設定範囲が広がる時は、その範囲について「追加登録」のルールが、狭くなる時は、その範囲にについて「削除」のルールが適用される。

(b) 専攻 IP 割当範囲

専攻割当範囲について「追加登録」、「削除」、「範囲の変更」を行う時、それぞれ次のチェックを行う (図 3. を参照)。

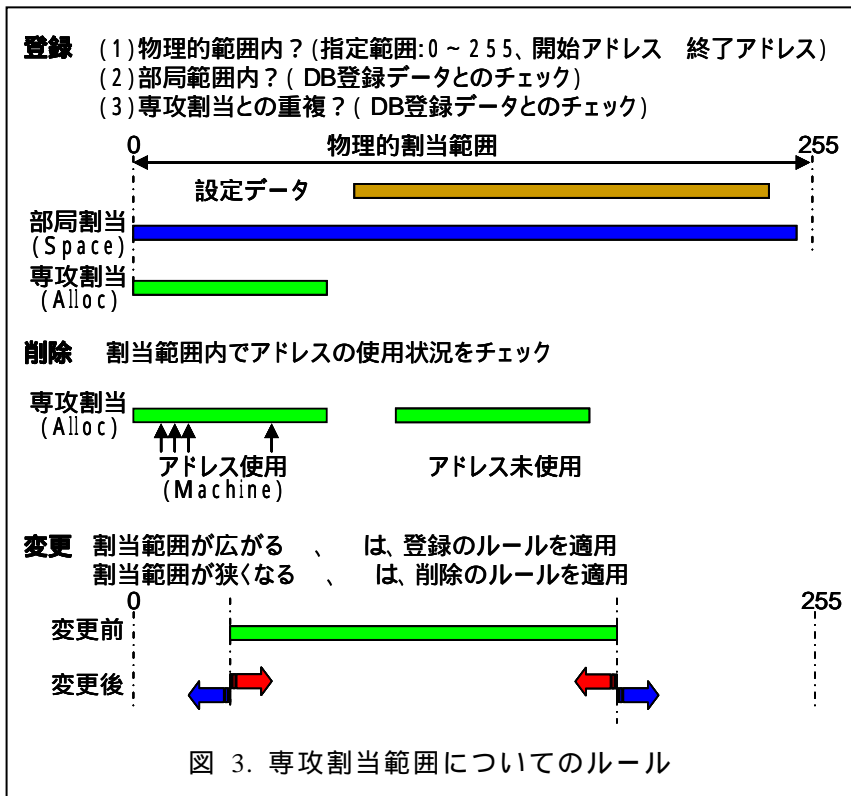
追加登録：設定した割当範囲について、(1) 物理的割当の範囲内であること、(2) 工学研究科の割当範囲内 (Space) であること、(3) 他の専攻割当 (Alloc) と重複していないこと、の3つについてのチェックが行われる。全ての条件を満足した時、この追加登録が実行される。

削除：削除する専攻割当 (Alloc) の範囲内に、端末情報 (Machine) データが登録されているかどうかの確認を行う。その範囲内のアドレスが使用されていない時はデータベースからの削除が実行され、アドレスが使用されている時は削除が拒否される。

範囲の変更：変更後の開始アドレス値、及び終了アドレス値が、それぞれ小さくなる場合と大きくなる場合の4つのケースが考えられる。

図 3. に示すように、

と の様に割当範囲が広がる場合については「追加登録」のルールが、 と の様に割当範囲が狭くなる場合については「削除」のルールが適用される。



3.3. メンテナンスシステム

本メンテナンスシステムにアクセスすると、ログイン画面が表示されるので、ここで管理者の ID、パスワードを入力する。ユーザー認証に成功すると、メニュー画面が表示されるので、必要なメンテナンス機能を選択する。

使用例として、専攻割当についての説明を以下に記述する。

(1) 専攻割当一覧 (図 4. 参照)

メニューの「IP 割当」を選択すると、現在登録されている割当範囲の一覧が表示される。一覧の下に表示された「登録」を選択すると (2) 専攻割当の追加登録へ、右端の「削除」を選択すると (3) 専攻割当の削除へ、「編集」を選択すると (4) 専攻割当の編集へ、リンク設定されている。

(2) 専攻割当の追加登録 (図 5. 参照)

専攻割当の登録設定は、専攻名と建物名についてはチェックボックスから選択、IP アドレス範囲として数値で入力する。後は、3.2. (b) 専攻 IP 割当範囲の追加登録のルールに従って登録が実行 (or 拒否) される。

(3) 専攻割当の削除 (図 6. 参照)

専攻割当の削除設定は、登録範囲がチェックボックスとして表示されるので、その IP アドレス範囲を選択する。後は、3.2. (b) 専攻 IP 割当範囲の削除のルールに従って削除が実行 (or 拒否) される。

(4) 専攻割当の編集 (図 7. 参照)

選択した専攻割当の設定値が表示されるので、テキストボックスに変更後のアドレスを指定する。後は、3.2. (b) 専攻 IP 割当範囲の範囲の変更のルールに従って編集が実行 (or 拒否) される。

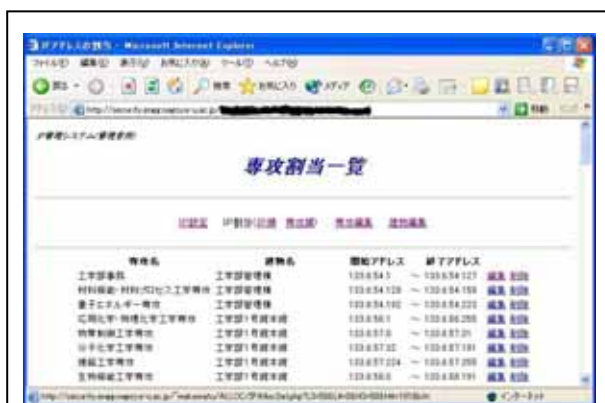


図 4. 専攻割当一覧



図 5. 専攻割当の追加割当



図 6. 専攻割当の削除



図 7. 専攻割当の編集

結果

今回構築したメンテナンスシステムを利用することにより、工学研究科の IP アドレス管理システム運用上に必要なデータベースの設定は、管理者としてのアカウント（管理者 ID とパスワード）さえ取得すれば、誰でも簡単、かつ正確に設定することができるようになった。

ここで、テーブルデータを設定する方法として、従来の方法と今回作成したメンテナンスシステムとの比較を表 5. に示す。

表 5. メンテナンスシステムと従来の方法との比較

	従来 の 方法	メンテナンスシステム
設定方法	データベースサーバーに接続する。	Web 上から行う（簡単な操作で行うことができる）。
入力方法	必要な sql 文を実行する必要がある（データベースの知識が必要となる）。	入力候補としてのリストボックスからの選択と、数値で指定する（誰でも設定が可能である）。
データの整合性	設定者自身が確認しなければならない（設定ミスが起きる可能性がある）。	プログラム内で設定したルールが判断する（設定ミスを起こすことがない）。
設定作業場所	データベースサーバー、及びアクセスを許可された端末からしか設定が出来ない。	学内の LAN に接続されている端末なら、どこからでも設定が可能である（パスワードが必要）。

まとめ

今回の研鑽研修において、

- (1) 構築した「IP アドレス管理用メンテナンスシステム」を利用することにより、誰でも正確に IP アドレスの割当が可能となったこと、
- (2) このことにより、IP アドレス管理については、設定の容易化と、当初予定していた人的バックアップを構築することが出来たこと、
- (3) 初心者と一緒にプログラム開発することにより、プログラミングの知識を持つ技術職員の拡充が出来たと考えている
- (4) 新しい言語である PHP についての知識を得ることが出来た

という様に、当初の研鑽研修の目的を達成することができた。

参考文献

- [1] 西沢直木, “PHP による Web アプリケーションスーパーサンプル,” ソフトバンク
- [2] 高島優作, “PostgreSQL7/PHP5 による Web アプリケーション構築,” 秀和システム
- [3] PostgreSQL Global Development Group 著 (日本 PostgreSQL ユーザー会、株式会社 SRA 訳), “PostgreSQL オフィシャルマニュアル,” インプレス
- [4] Nicolai Langfeldt 著 (竹内里佳訳), “DNS & BIND 入門,” オーム社