# RADIUS／LDAPと連携したMACアドレス認証システムの構築

石井, 大輔
九州大学応用力学研究所

https://doi.org/10.15017/2329127

出版情報：九州大学応用力学研究所技術室 技術室報告. 1, pp.56-59, 2019-07. Research Institute for Applied Mechanics, Kyushu University
バージョン：
権利関係：

九州大学応用力学研究所 技術室
技術室報告 Vol. 1, 56-59

# RADIUS／LDAP と連携した MAC アドレス認証システムの構築

石井　大輔

**要　旨**

応用力学研究所では、機器情報一元管理システム（SECURE.RIAM）の構築と同時に導入した MAC アドレス登録制が運用されて早 10 年が経過しようとしている。今まで特段のトラブルもなく運用されてきたが、更なる技術的課題の解決に取り組むため、今回 RADIUS 機能と LDAP 機能を融合し既存システムと連動させた、MAC アドレス認証システムを新たに構築した。

**キーワード**

MAC アドレス　認証　RADIUS　LDAP

## 1．はじめに

MAC アドレスとは、通信ネットワーク上で一意に識別するため物理的に割り当てられた 48 ビットの識別番号のことであり、16 進数で「xx-xx-xx-xx-xx-xx」「yy:yy:yy:yy:yy:yy」と表される。物理アドレスと呼ばれることもある。

当研究所では、2010 年に機器情報一元管理システム（SECURE.RIAM）の構築と、MAC アドレス登録制の導入により、今まで以上にセキュアな所内ネットワーク環境を整備した[1]。IP アドレスを自動割り当てする DHCP 運用では、未登録の不特定機器（部外者の端末、所有者が把握できないウイルス感染端末など）による所内ネットワーク接続が不可になったことで、セキュリティリスクとインシデント事案の発生が大幅に低減した。また、研究所全体のネットワーク管理者（計算機室）や各研究室のネットワーク管理者にとって、運用コストや管理コストが格段に軽減された。

DHCP による IP アドレスの自動割り当てをしない通信機器もある。プリンタや計算サーバ等、他所からのネットワーク接続があり得る通信機器に対しては、計算機室から一意の固定 IP アドレスを割り当て、それをクライアント（利用者や研究室ネットワーク管理者）が当該機器に手動で設定する運用である。

MAC アドレス登録制を導入してから、DHCP の場合は、登録された MAC アドレスによって DHCP クライアントをシステム側で識別して IP アドレスが割り当てられるため、任意の IP アドレスが付与される DHCP 端末でも簡単に特定することができた。しかし、固定 IP の場合は、機器情報を基に IP アドレスを手動で割り当てているため、機器特定の面ではそこまでのシステム開発は必要なかった。加えて、当時は開発技術の難度や開発工数の不足、必要関連機器の新規整備など、技術面や費用面等の制約もあってのことから、更なる開発・改修には踏み込まなかった。

その後現在までに、固定 IP 運用に係るトラブル事案が何度か発生した。それは、割り振られた固定 IP アドレスの競合による通信不調である。通信機器へのネットワーク情報の設定は利用者が行うことが専らであるが、パソコン関係にあまり詳しくない者も少なくないため、設定時の人為的ミスが生じやすい。当然、その人に割り当てられた固定 IP アドレスではないので他人と競合して通信不調が生じる（一次被害）。悪意があっての所作ではないので咎められないが、どこで、どの端末によって引き起こされているのか、その特定には時間を要することが多かった（通信できる時もあるので）。その間、正規に当該固定 IP アドレスを使用している利用者にとっては、心当たりが無い状況で IP 競合のアラート出現と通信不調が不定期に生じるので、業務等に支障（二次被害）が出てしまっていた。

他にも理由はあるのだが、大きくは既述の事案を技術的に解消するため策を講じる必要があった状況で、運よく必要関連機器（レイヤー2 インテリジェントスイッチ : L2 スイッチ）を調達できる機会に恵まれたため、現システムの改修と新たな仕組みを導入したシステムとして、RADIUS／LDAP 機能を連携させた MAC アドレス認証システムを構築するに至った。

## ２．MAC アドレス認証システムの構築

RADIUS （ Remote Authentication Dial In User Service）とは、ネットワーク上のユーザ認証プロトコルのことで、有線 LAN・無線 LAN を問わず、ネットワーク接続時のユーザ認証に利用されている。数十年前から活用されており、電話回線を使ったダイヤルアップ（DUN）接続がその代表例である。また、LDAP （Lightweight Directory Access Protocol）とは、ディレクトリサービスへアクセスするためのプロトコルのことで、他には AD（Active Directory）などが有名である。今回開発するにあたり、現在当研究所の計算機室で運用中のシステム・サービスを拡張するイメージで構想を検討した。

表 1 に、本システムを構築する上で必要となったサーバ構成を示す。同表内のサービスにおける M, S の表記は、Master, Slave の意である。既に、研究所システムとして LDAP サービスと DHCP サービスは仮想マシン 2 台（Red Hat Enterprise Linux）で稼動しているため、これらに RADIUS サーバを構築し、サービスの冗長を図った。表 2 には使用したソフトウェアの仕様を示しており、今回は OSS（オープンソースソフトウェア）として導入実績が多く動作が安定している、FreeRADIUS [2]と OpenLDAP [3]を採用した。

図 1 に、新たに構築した MAC アドレス認証システムの概要と認証シーケンスの模式図を示す。以下の設定条件の下でどのような動作になるのか、時系列で簡単に説明する。

【利用者が使用する通信機器に係る条件例】

・有線 LAN アダプタを使用

・DHCP による自動割り振りではなく、固定 IP アドレスを設定したい

MAC アドレス認証システム　外

・利用者は同端末の有線ネットワークポートに LAN ケーブルを挿し、他端を所内ネットワークに繋がるスイッチングハブ等のポートに挿して、接続開通できるかを試行する。

・しかし、当該マシンへの固定 IP アドレスが割り振られていない状況なので、通信できない。

・そこで、当該マシンで使用している NIC（Network Interface Card）の MAC アドレス情報を研究室ネットワーク管理者に知らせ、SECURE.RIAM への登録申請を依頼する。

MAC アドレス認証システム　内

・申請依頼に対し、計算機室での承認手続きが完了したら、当該マシンに割り振る「固定 IP アドレス」と「MAC アドレス」情報が対として自動的に LDAP サーバへ登録される。

・サーバ A, B の LDAP サービスは同期させているので、上記の情報は両サーバに登録される。

MAC アドレス認証システム　外

・利用者は研究室ネットワーク管理者から「固定 IP アドレス」を教えてもらい、利用マシンにネットワーク情報として設定する。設定後、接続が開通されるか再度試行する。

MAC アドレス認証システム　内

・MAC アドレス認証が設定された制御スイッチ（L2 スイッチ）のところで、MAC アドレステーブルに当該マシンの MAC アドレス情報が登録されているか、判定が入る。

・テーブルに登録がなければ、RADIUS サーバに MAC アドレス認証を要求する。

・RADIUS サーバで認証が成功すれば、その認証結果が L2 スイッチの MAC アドレステーブルに反映され、MAC アドレスが登録される。

MAC アドレス認証システム　外

・その後、MAC アドレス認証が成功し、利用者は当該マシンでの対外通信ができるようになる。

表 1　開発システムにおけるサーバ構成

| サーバ構成 | OS | サービス |
|---|---|---|
| A（仮想マシン） | Red Hat Enterprise Linux 6 | RADIUS , LDAP (M), DHCP (M) |
| B（仮想マシン） | Red Hat Enterprise Linux 6 | RADIUS , LDAP (S), DHCP (M) |

表 2　サービスのソフトウェア構成

| ソフトウェア構成 | バージョン | サービス |
|---|---|---|
| FreeRADIUS | freeradius-2.2.6-7.el6_9.x86_64 | RADIUS |
| OpenLDAP | openldap-2.4.40-16.el6.x86_64 | LDAP |
| DHCP | dhcp-4.1.1-63.P1.el6_10.x86_64 | DHCP |

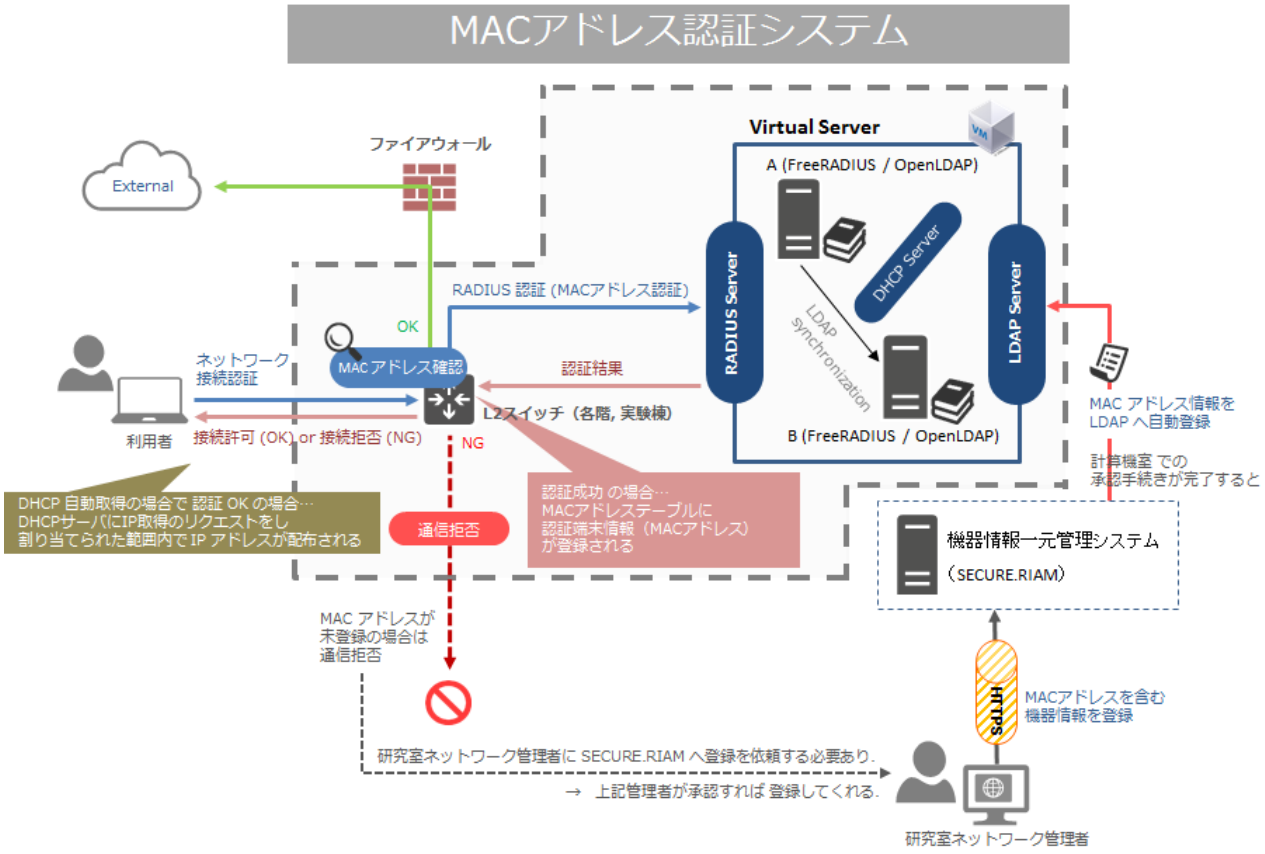


図 1　MAC アドレス認証システムの概略図・認証シーケンス

前述は「固定 IP アドレス」であったが、DHCP による IP アドレス自動取得の場合は、L2 スイッチの MAC アドレステーブルが更新された時点で、認証後の VLAN に切り替わり（説明は省略）、DHCP サーバへ IP アドレスの取得要求をし、DHCP サーバから IP アドレスが自動で割り振られるシーケンスとなる。

## 3．おわりに

紙面の都合と安全上の観点から本件に係る技術的な詳述は控えさせて頂くが、現在まで特段の問題なく本システムは運用できている。運用当初は、SECURE.RIAM 申請後、計算機室から開通許可が下りたのに所内ネットワークが繋がらない、DHCP で IP アドレスを自動取得したのに対

外通信できない、などの連絡が少なからず寄せられていた。調べてみたところ、それらの原因の大半は SECURE.RIAM へ登録した（利用者が研究室ネットワーク管理者に伝言した）MAC アドレス情報と、利用者が実際に使用している通信デバイスにおける NIC の MAC アドレス情報が異なっていたことだった。MAC アドレスは、有線や無線、カード型や USB 型などの別に関係なく、NIC それぞれに固有の値が設定されているため、利用者が調べた際に間違えて別のネットワークアダプタの MAC アドレス値を伝言してしまったことが主な要因と考えられる。

ただこのことから、登録情報と実際における NIC の MAC アドレスが一致しないと技術的に通信が許可されない挙動になることを改めて確認することができた。それは即ち、素性が分からない通信機器を所内ネットワーク網へ持ち込み物理的に結線させたとしても、様々な認証が通らないと正規利用ができないことを意味している。

本システムの構築と運用が、研究所におけるセキュアなネットワーク環境の維持管理に少なからず貢献できていれば幸いである。

## 参考文献

[1] 松島啓二・石井大輔：ネットワーク機器およびメール／計算機ユーザの登録・管理システム構築, 九州大学応用力学研究所技術室 技術レポート, 12, 63-71, 2011.
[2] FreeRADIUS：https://freeradius.org/
[3] OpenLDAP：https://www.openldap.org/

## 謝辞

本開発を進める上で必要が生じた既存システム SECURE.RIAM の一部改修にあたり、技術職員の松島啓二氏から技術支援を頂きました。この場をお借りして、感謝の意を表します。