Vol.2022-IOT-56 No.25
2022/3/8

ネットワーク接続機器用アカウントの発行サービス構築と運用

針木 剛[1,a)]　中村 素典[1,b)]

概要：京都大学では無線 LAN サービスや有線接続での Web 認証付き情報コンセントサービスを行っているが接続には教職員や学生などの大学構成員個人に紐付く全学アカウントを必須としている．特に無線 LAN サービスでは複数人で利用するタブレットや複合機などの共用デバイスにも全学アカウントが必要なため，複数人による全学アカウントの使いまわしなどの問題があった．本論文ではその対策として既存システムに機能を付与して教職員自身が接続機器用アカウントを発行できるサービスの構築を行ったのでその具体的な内容を紹介する．またそのサービスの運用方法や導入時の問題点，今後の課題などに関して詳細に述べる．

キーワード：無線 LAN，Web 認証付き有線 LAN，機器アカウント，MAC アドレス制限

1. はじめに

京都大学では構成員が講義室や会議室や図書館等の共有スペース，複数の居室や研究室に隣接する廊下などを中心に無線 LAN アクセスポイントを設置して無線 LAN サービスを提供している．また共有スペースにおいて，より安定した遠隔配信のため有線 LAN 接続においてブラウザでのパスワード認証で利用可能な Web 認証付き情報コンセントサービスを提供している．

これらサービスの利用にはすべての大学構成員に個別発行される全学アカウントが必須となるが，例えば複数人で共有するタブレット端末や複合機，IoT デバイスなどを無線 LAN サービスに接続しようとした場合にも全学アカウントが必要となる．全学アカウントは学内の多くの個人情報電子リソースと結びついており，使いまわしによる情報漏洩の懸念があることから個人のアカウントとは異なる認証方法について各所から要望が挙がっていた．

また公共的に利用されるホールなどの施設では学外者へのネットワーク接続サービスも必要となる．無線 LAN については国立情報学研究所による eduroamJP の認証連携 ID サービスで提供されるビジターアカウントで対応しているが，有線 LAN については学外者のための接続用アカウントは提供できていなかった．

[1] 京都大学 Kyoto Uniersity
[a)] hariki.tsuyoshi.3r@kyoto-u.ac.jp
[b)] nakamura.motonori.2c@kyoto-u.ac.jp

本稿では，それら無線 LAN サービスや Web 認証付き情報コンセントサービスで利用可能となる接続機器用アカウントの発行システムの構築と，実際にそのサービス運用を行った際に生じた問題点や利用者からの要望，今後の機能追加に関して詳細に述べる．

2. 学内ネットワークサービスの詳細

2.1 ネットワーク管理データベース

京都大学の学術情報ネットワークシステム（Kyoto University Integrated information Network System, 略称:KUINS）では学内構成員が研究室 VLAN でパソコンやプリンタを利用するためのプライベート IP アドレス「KUINS-III」と、学外への通信や学外公開のためのグローバル IP アドレス「KUINS-II」を運用している。

京都大学ではそれら KUINS-II 及び KUINS-III のネットワーク情報を一元管理する「KUINS-DB」と呼ばれるデータベースシステムを 2002 年より運用している．[1], [2]

教職員は KUINS-DB の Web フォームから希望する KUINS-II の IP アドレスや MAC アドレス，KUINS-III のサブネットサイズや DHCP の範囲，利用したい研究室や居室の情報コンセント名などの申請を行う．受理された申請内容に VLAN 情報やゲートウェイ機器情報等を付加したデータベースの内容をネットワーク機器の設定に変換し，各機器へ自動的に投入することで全学ネットワークの運用を行っている．

KUINS-III では研究室や係といった組織単位で VLAN

を細分化し，基本的に異なる VLAN へは接続不可として運用している．また VLAN を識別するために「VLAN 管理番号」の名称で 5 桁以上の数字を割り当てて管理している．

2.2 無線 LAN サービス

学内の共有スペースには無線 LAN アクセスポイントを設置しており「全学アカウント」を用いて 802.1X 認証で利用する学内構成員用の無線 LAN サービスを提供している．通常は認証後に共通の KUINS-III の VLAN に接続しインターネット接続だけでなく学内の各種電子リソースが利用できるようになる．このサービスではさらに接続認証時に ID を「全学アカウント@VLAN 管理番号」とすることで研究室などの閉じた VLAN に L2 接続できるような機能も提供している．[3]

利用の際には KUINS-DB にて VLAN 管理者である教職員がその VLAN に接続可能な全学アカウントの登録申請を行うと無線 LAN コントローラや無線 LAN 用 radius サーバ等に設定が反映され利用することが可能となる．

2022 年 1 月現在 KUINS-III の VLAN は全学で約 4,000 個利用されており，そのうち約 900 個の VLAN で研究室への直接接続機能を利用されている．これらの各構内の約 900 の VLAN を集約し，無線 LAN コントローラにタグ VLAN として出力している．

2.3 Web 認証付き情報コンセントサービス

研究室や事務室などと異なりホールや講義室や会議室のような不特定多数の学内関係者が入退室するようなスペースでの情報コンセントではブラウザで認証して利用できる Web 認証付き情報コンセントサービスを提供している．

利用者は「全学アカウント」を用いて認証するが，認証は無線 LAN 用の radius サーバと共用している．したがって新たなアカウントサービスを同一 radius サーバで実装することで両サービスに対応可能である．

また学内の各情報コンセントに対し約 900 のタグ VLAN の出力は難しいため研究室に直接接続できるサービスは行っていない．

2.4 VPN サービス

学外から学内の電子リソースを利用するために VPN サービスを提供している．主たる IKEv2 サービス [4] と IPsec が利用不可なネットワーク環境のための補助的な OpenVPN サービス [5] の 2 種類のサービスを提供している．また学外公開サービスのためパスワード認証ではなくクライアント証明書認証を推奨している．

無線 LAN サービス同様「全学アカウント」で認証すると共通の KUINS-III に接続し学内共通のリソースが利用でき，また「全学アカウント@VLAN 管理番号」で認証するとクライアントからの通信を VPN サーバ内で研究室などの VLAN の IP アドレスに NAT することで，閉じた研究室の電子リソースにも接続できる機能を提供している．

こちらも集約された研究室 VLAN を学内の仮想化基盤上に構築された仮想マシンで稼働する VPN サーバに出力することでサービスが提供可能となっている．

3. 接続機器アカウントサービスの構築

要望のあった無線 LAN サービス及び Web 認証付き情報コンセントについて，接続機器アカウントの発行機能の実装と両サービスの radius サーバの設定変更を行った．

新たな接続機器アカウントに関して以下の機能を検討した．

(1) 使い回しを制限するため機器への紐づけ
(2) 複合機や IoT 機器を利用するため個々の研究室 VLAN へ接続する機能
(3) 未使用アカウントを適宜削除させる動機づけ

ここで Web 認証付き情報コンセントサービスの場合は研究室 VLAN へ接続する機能を提供していないため，Web 認証付き情報コンセントに限り (2) の機能は対象外とした．

3.1 KUINS-DB 申請フォーム改修

アカウント申請するための Web フォームは新たな Web システムを構築するのではなく，既存の KUINS-DB システムを改修することで対応した．要求機能 (2) のためアカウントは利用する VLAN 情報に紐づける必要があるが，KUINS-DB で利用されている VLAN 申請フォームに新たに VLAN の属性項目の一つとして接続機器アカウントを登録申請できるよう改修を行った．

KUINS-DB で管理している VLAN 情報の一部と新たに追加した項目を表 1 にまとめる．

表 1 KUINS-DB で管理する VLAN 情報

VLAN 管理番号	12345
管理責任者	名前：○○
	連絡先：xxx.xxx.xx@kyoto-u.ac.jp
支払費目	運営費-研究-教育研究事業費
ネットワークアドレス	10.0.0.0/24
DHCP アドレス範囲	10.0.0.10 - 10.0.0.240
VLAN 番号	100（集約時 1000）
情報コンセント	A 棟 101 室 101-a
	A 棟 102 室 102-a
全学アカウント	ID1
	ID2
:	:
接続機器アカウント*1	34-E1-2D-XX-XX-XX k12345-1, secret1, 10.0.0.241
	A0-4E-A7-XX-XX-XX k12345-2, secret2, -

*1) 新規追加項目

要求機能 (1) に関しては radius の認証時に特定の MAC

アドレスを持つ機器だけが特定の ID とパスワード認証できるよう設定を行う．そのためアカウント申請時には機器の MAC アドレスを必須入力とし，申請処理時には自動でその MAC アドレスに対応する ID とパスワードを発行するよう機能追加を行った．入力画面では多量の MAC アドレス入力を容易にするため，個別入力に加えエクセルファイルでの一括入力にも対応した．これら KUINS-DB に登録された MAC アドレスと ID とパスワード情報は，定期的に radius サーバに反映するようバッチ処理を設定した．

また機器に対し固定 IP アドレスを設定したいといった要望に備え，任意入力欄として IP アドレスの項目を用意した．本学の無線 LAN システムでは DHCP による IP アドレス割り当てを必須としているため，端末側で手動で IP アドレスを設定するのではなく DHCP サーバが常にその IP アドレスを割当てるよう設定を行う．したがってそれら申請された MAC アドレスと IP アドレスは別途 DHCP サーバへの設定追加処理とした．

このようにアカウントを個人ではなく VLAN に紐づけることで，VLAN 管理者である教職員の異動や退職時にも，VLAN 情報の引き継ぎだけでアカウントや情報コンセントなどの研究室のネットワーク情報がすべて一括で引き継ぐことが可能である．

3.2 radius サーバの MAC アドレス認可機能

京都大学では radius サーバとして学内の仮想化基盤上に構築された仮想マシンにて RedHatEnterpriseLinux7 にバンドルされた freeradius-3.0.13 を利用している．

また接続機器アカウントの体系は VLAN 管理番号に通し番号を付与しレルム固定の「k[VLAN 管理番号]-[通し番号]@ka」としている．レルムの「ka」は「全学アカウント@VLAN 管理番号」の VLAN 管理番号と重ならない固定文字列とした．

なお「全学アカウント@VLAN 管理番号」の機能は「files」モジュールで処理しており，新たに「files_ka」を次のように定義した．

```
--/etc/raddb/mods-enabled/files--
files files {
    ...
}
files files_ka {
    moddir = ${modconfdir}/${.:instance}
    filename = ${moddir}/authorize
    acctusersfile = ${moddir}/accounting
    preproxy_usersfile = ${moddir}/pre-proxy
}
```

```
--/etc/raddb/mods-config/files_ka/authorize--
DEFAULT
    Tunnel-Type = "VLAN",
    Tunnel-Medium-Type = "IEEE-802",
    Fall-Through = Yes

k12345-1 Cleartext-Password := "secret1",
    Calling-Station-Id == "34-E1-2D-XX-XX-XX"
    Tunnel-Private-Group-Id = "1000"
k12345-2 Cleartext-Password := "secret2",
    Calling-Station-Id == "A0-4E-A7-XX-XX-XX"
    Tunnel-Private-Group-Id = "1000"
k12346-1 Cleartext-Password := "secret3",
    Calling-Station-Id == "98-01-A7-XX-XX-XX"
    Tunnel-Private-Group-Id = "1001"
```

例えば MAC アドレスが 34-E1-2D-XX-XX-XX の機器が ID を k12345-1 で接続してきた場合に secret1 のパスワードで認証し VLAN 番号 1000 を返す設定となる．それ以外の MAC アドレス機器が k12345-1 で接続した場合は認証エラーとなる．この「authorize」ファイルの情報は定期的に KUINS-DB から取得し更新している．

また「files_ka」を機能させるため次の設定を追加した．

```
--/etc/raddb/sites-enabled/default--
authorize {
    ...
    rewrite_calling_station_id
    if (User-Name =~ /^[^@]+@ka$/) {
        files_ka
    }
    files
    -ldap
    if (Client-Shortname == "swauth") {
         update reply {
             Tunnel-Private-Group-Id := ""
         }
    }
    ...
}
```

```
--/etc/raddb/sites-enabled/inner-tunnel--
server inner-tunnel {
authorize {
    :
    if (User-Name =~ /^[^@]+@ka$/) {
        update request {
            &Calling-Station-Id :=
            &outer.request:Calling-Station-Id
        }
        files_ka
    }
    files
    -ldap
    if (Client-Shortname == "swauth") {
         update reply {
             Tunnel-Private-Group-Id := ""
         }
    }
    :
}
}
```

「default」では「rewrite_calling_station_id」で MAC アドレス表記を正規化しており，また「inner-tunnel」には MAC

アドレスの属性情報が存在しないため「Calling-Station-Id」を別途追加している．

さらに「swauth」と名付けた Web 認証付き情報コンセントのクライアントからの要求には VLAN 番号を返さないような設定をしている．

4. サービス運用時の問題点

京都大学では「KUINS 接続機器アカウント」として 2021 年 7 月よりサービスを開始し，2022 年 1 月現在で約 1,800 アカウント，約 90VLAN で利用されている．問い合わせ内容から共有タブレット機器で多く利用されていると思われる．以下に実運用にて利用者から多く頂いた問い合わせや要望をまとめる．

4.1 ランダム MAC アドレスの無効設定

マニュアル等にてランダム MAC アドレスの無効化を必須としているが，未設定で利用開始した複数の利用者から認証不可となるといった問い合わせを頂いている．約 7 ヶ月間で 10 件未満の問い合わせ数ではあるが，増えるようであればマニュアルやよくある質問以外の通知方法も検討する必要がある．

4.2 DHCP 未使用設定

KUINS-DB では VLAN の設定で DHCP アドレス範囲を設定可能であり，DHCP での利用可能 IP アドレスをゼロとして接続機器アカウントを申請されるケースが 1 件あった．実際の利用で接続不可となったため発覚したが，DHCP が必須である旨マニュアルに追記して対応した．

4.3 MAC アドレスのメモ欄

申請した MAC アドレスがどのような機器であるか管理するためのメモ欄の要望があり，改修を検討中である．

5. 補助機能

5.1 MAC アドレスと IP アドレス履歴情報の提供

申請済みの MAC アドレスが利用中かどうか確認するために 2021 年 12 月より MAC アドレスの履歴情報の提供を行っている．

1 時間ごとに定期的に VLAN のゲートウェイである L3 スイッチ機器にログインして IPv4 の ARP 情報や IPv6 の Neighbor 情報を取得して KUINS-DB に登録している．

VLAN 管理者が KUINS-DB にログインするとその VLAN に接続した MAC アドレスの IP アドレス，初回検知日時，最終接続日時について過去 1 ヶ月分が閲覧可能となっている．本機能は KUINS 接続機器アカウントの機器だけでなく VLAN を利用するすべての機器の履歴が確認できるため，VLAN 接続機器一覧を定期的に確認するツールとして利活用も可能である．

6. 追加予定機能

6.1 負担金請求機能

要求機能 (3) の方法として個々の接続機器アカウントについて負担金請求機能の実装を検討している．

現在 KUINS-DB では VLAN に関して情報コンセント数に応じた負担金請求を行っており，そのため KUINS-DB の VLAN 情報には予算費目などの経理情報も登録済みである．これらの情報を用いることで負担金請求機能の実現が可能と考えている．

6.2 クライアント証明書発行機能と VPN サービスへの展開

KUINS 接続機器アカウントに自動でパスワードを付与しているが，無線 LAN だけでなく学外からの VPN 接続に対応するため，より安全なクライアント証明書発行機能を検討している．

特に外部業者が研究室内のサーバを遠隔からメンテナンスするための VPN アカウントの要望も挙がっている．VPN 利用者が業者であるため，学内構成員用の VPN サービスで提供しているような学内すべてに接続できる環境ではなく，接続先をメンテナンス機器が設置してある研究室 VLAN にのみ限定したサービスであることが望ましい．

また証明書の安全でかつ使い回しを抑制するような業者への提供方法も課題と考えている．

7. まとめ

- ネットワーク接続機器用アカウントの発行サービス構築を行い，約 7 ヶ月運用を行った．
- アカウントは使い回しを防ぐため利用機器の MAC アドレスを限定し，無線 LAN サービスにおいて各研究室の VLAN に直接接続できる機能を備えた．
- 今後利用者からの問い合わせや要望などをもとに，申請フォームやマニュアルの微修正に加え新たな機能追加も検討している．

参考文献

[1] 宮崎修一 他：KUINS 接続機器登録データベースの概要，第２７回全国共同利用情報基盤センター研究開発連合発表講演会 研究開発論文集 pp.47-51 (2005)
[2] 高見好男 他：京都大学学術情報ネットワークシステム接続機器管理システム『KUINS-DB 』の更新，第３４回全国共同利用情報基盤センター研究開発連合発表講演会 研究開発論文集 pp.53-57 (2012)
[3] 針木剛：全学無線 LAN での研究室 VLAN 接続サービスの構築，総合技術研究会 2017 東京大学
[4] 針木剛：京都大学における IKEv2 サービスの構築，2016 年度大学 ICT 推進協議会年次大会
[5] 針木剛：OpenVPN を用いた個別 VLAN 接続サービスの構築，2020 年度大学 ICT 推進協議会年次大会