キャンパスネットワークにおける全学的なネットワーク認証の導入

大森 幹之 [1)]

1) 鳥取大学 総合メディア基盤センター

ohmori@tottori-u.ac.jp

A Network Authentication in a Whole Campus Network

Motoyuki OHMORI[1)]

1) Center for Information Infrastructure and Multimedia, Tottori University

概要

鳥取大学では，2005 年度より全新入生に対してノート PC の必携を求めており，BYOD (Bring Your Own Device) を推進してきた．この環境では，セキュリティインシデントや障害などの発生時に，原因となっている端末を特定するために，ネットワークに接続する端末の認証（ネットワーク認証）が重要である．無線 LAN に関しては一般的となった IEEE802.1x 認証を導入していた．一方，有線 LAN に関しては IEEE802.1x 認証が一般的でない，Web 認証のスイッチの負荷が高い，Web 認証時に SSL/TLS の証明書エラーが生じるなどといった課題のためにネットワーク認証を導入できていなかった．そこで，2018 年度 4 月より，Captive Portal の実装，Microsoft Windows OS が IEEE802.1x 認証をデフォルトで有効化したことなどにより，シームレスに教育用ネットワークで全学的にネットワーク認証を実装できた．本論文では，全学的にネットワーク認証を導入するにあたって得られた知見について報告する．

1 はじめに

鳥取大学では，2005 年度より全新入生に対してノート PC の必携を求めており, BYOD (Bring Your Own Device) を推進してきた．この環境では, セキュリティインシデントや障害などの発生時に，原因となっている端末を特定するために，ネットワークに接続する端末の認証（ネットワーク認証）が重要である．鳥取大学では，無線 LAN に関しては一般的となった IEEE802.1x 認証を導入していた．一方，有線 LAN に関しては IEEE802.1x 認証が一般的でない，Web 認証のスイッチの負荷が高い，Web 認証時に SSL/TLS の証明書エラーが生じるなどといった課題のためにネットワーク認証を導入できていなかった．そこで，2018 年度 4 月より, Captive Portal の実装, Microsoft Windows OS が IEEE802.1x 認証をデフォルトで有効化したことなどにより，シームレスに教育用ネットワークで全学的にネットワーク認証を実装できた．本論文では，全学的にネットワーク認証を導入するにあたって得られた知見について報告する．

以降の本稿の構成は以下のとおりである．**2 節**においてネットワーク認証を全学的に実装するための課題について述べる．**3 節**においてネットワーク認証を実装した鳥取大学のネットワークの概略について述べる．**4 節**，**5 節**において鳥取大学で実装したそれぞれ無線 LAN，有線 LAN におけるネットワーク認証について述べる．**7 節**において，開発中の Windows OS 向けの IEEE802.1x 認証の設定を自動化するツールについて述べる．最後に **8 節**において，本稿をまとめる．

2 ネットワーク認証の課題

ネットワーク認証が重要であることには疑いの余地はないが，様々な要因により全学的に展開するには解決すべき課題があると考えられる．本節では，ネットワーク認証を全学的に展開する際に課題となる点について述べる．

2.1 IEEE802.1x 認証の実装の違い

なりすましや MITM（Man-In-The-Middle）攻撃の防止といった安全面や認証に要する時間といったパフォーマンスの観点から，技術的にはネットワーク認証の中では IEEE802.1x 認証が最適であると考えられる．しかし，各 OS での実装に違いがあり，その違いが運用を難しくしている．**表 1** に各 OS での実装の違いを示す．**表 1** に示される様に，PKI のトラストアンカーの設定は，macOS では，キーチェインアクセスと呼ばれるアプリケーションや iCloud キーチェインで管理され OS 全体で共通である．そして，ルート認証局を一旦信頼すれば，有線 LAN の NIC や無線 LAN

の SSID 毎に信頼するルート認証局を設定する必要がない．一方，Windows OS では有線 LAN の NIC や無線 LAN の SSID の設定毎に信頼するルート認証局を設定しなければならず，利用者が安全な設定をすることが困難になっている．

また，IEEE802.1x 認証をより安全にするために，認証時の RADIUS サーバを明示的に設定することが望ましい．しかし，macOS では GUI から容易に設定できず，EAPClientConfiguration 辞書へ登録する特別な設定が必要となる [1]．そのため，一般的な利用者が設定するのは困難である．一方，Windows OS では GUI から設定できる．しかし，RADIUS サーバの FQDN の入力間違いや複数の RADIUS サーバを設定する際に「;」（セミコロン）をマルチバイト文字で入力するなどの誤操作を完全には防止できない．その上，誤操作により誤った設定にした場合には，設定画面を一旦閉じてしまうと再度設定することができなくなる．その場合，設定を削除した後，再度設定しなければならない．これは，利用者にとっては大きな負担である．特に，情報機器の操作にあまり慣れていない利用者が誤操作を招くことが多いと考えられ，その様な利用者にとって RADIUS サーバの設定は大きな負担となっている．これらの理由から RADIUS サーバを明示的には設定しない場合も許容せざるを得ないと考えられる．

そして，有線 LAN における IEEE802.1x の設定について考察する．macOS では，IEEE802.1x 認証機能がデフォルトで有効になっている．そのため，RADIUS サーバの設定を除けば，アカウント情報の入力だけで設定を完了できる．一方，Windows OS では，**表 1** に示される様に OS のバージョンによって，IEEE802.1x 認証機能のデフォルトでの有効，無効の設定が異なる．特に，Windows 7 や Windows 10 の 1709 未満では，IEEE802.1x 認証機能を有効にせねばならず，その設定は一般的な利用者にとっては難しいものと考えられる．

上記の様に，OS に依存して IEEE802.1x の実装や設定が大きく異なる．そのため，利用者からの問い合わせに対応する者が OS に対してより深い知識を有していることが求められる．その結果，運用には高度な技術力を有した教職員が必要となり，全学的な展開が難しくなると考えられる．

2.2 Web 認証時の遅延と SSL/TLS 時の警告

Web 認証では，認証前の端末の HTTP や HTTPS の通信をスイッチが横取りし，認証のための Web ページにリダイレクトすることが多い．このリダイレクトの処理がスイッチに与える負荷は無視できない程に大きい．例えば，鳥取大学では Captive Portal を実装していない環境で，約 60 台の認証が完了するまでに，30 分以上要することが確認された．また，最悪の場合，10 台未満であっても認証が完了するまでに 30 分以上要することも観測された．これは，Windows OS が，IP アドレスを取得し Web 認証によって認証される前に，HTTP や HTTPS のポート番号の TCP コネクションを用いて Windows Update といったトラフィックを大量に生成することなどに起因していた．Windows Update のトラフィックのみ認証無しで通過させる対応も考えられるが，Windows Update のサーバの IP アドレスは変化することがあり，その変化に追従するのは現実的ではない．この様に，Windows Update などの認証前の大量トラフィックに起因する遅延は Web 認証の課題と言える．

また，認証前の HTTPS の通信を横取りする場合，FQDN が証明書内の CN の値と一致しないため，警告が Web ブラウザ上に表示されるか，通信ができなくなってしまう．例えば，2018 年 4 月時点の Microsoft Edge では，HTTPS での通信時に警告が表示されるページは開くことができなくなっており，認証の Web ページを表示できないのが現状である．そして，Google Chrome では 2018 年 7 月リリースの Chrome 68 から HTTP のページを「保護されていません」と警告が表示されてしまう．この様に HTTPS が必須となりつつある一方で，HTTPS では証明書の警告が防げず認証ページを表示できないこともあるという課題を抱えている．

2.3 複数 SSID による混乱と制御フレームの増大

鳥取大学での無線 LAN では，教育用，研究用，ゲスト用，TV 会議用，eduroam などの SSID を用意している．そのため，どの SSID を利用すれば良いか利用者が混乱する自体が発生している．また，IEEE802.11 の無線 LAN では，Beacon は 100msec であることが多く，SSID の数に比例して，最低レートのブロードキャストで送信される Beacon によって無線区間の送信時間が奪われてしまう．また，端末が基地局を発見するスキャンでは，端末が Probe Request をブロー

*1 Web ブラウザ，有線 LAN の NIC，無線 LAN の SSID 毎に異なる．

*2 Firefox といったサードパーティ製ブラウザの場合は別に設定が必要になることがある．

表 1　IEEE802.1x 認証の実装の違い

OS	共通		有線 LAN デフォルト設定	無線 LAN デフォルト設定
	PKI のトラストアンカー	RADIUS サーバ認証設定		
Windows 7	設定毎に別[*1]	GUI で可能	無効	有効
Windows 10 (1709 未満)	設定毎に別	GUI で可能	無効	有効
Windows 10 (1709 以降)	設定毎に別	GUI で可能	有効	有効
macOS	OS 全体で共通[*2]	GUI から不可	有効	有効

ドキャストで送信するため，無線区間の送信時間が奪われてしまう．特に，セキュリティの向上には貢献しない所謂ステルスの設定をしている SSID の場合にはより送信時間は失われる．これは，ステルスに設定された全ての SSID 対して，Probe Request を端末が一度に送信することに起因している．IEEE802.11ai TG においても環境によっては全トラフィックの全送信時間の半分以上を Beacon や Ack，Probe Request，Probe Reply といった制御フレームが占めることが示されている．これらのことから，SSID の種類は最小限に抑えることが望ましいと言える．

3　ネットワーク環境

本節ではネットワーク認証を導入した鳥取大学のキャンパスネットワークの構成について述べる．鳥取大学では，湖山キャンパス，米子キャンパス，浜坂キャンパスをメインキャンパスとして，附属フィールドサイエンスセンター，附属幼稚園，附属特別支援学校にキャンパスネットワークを敷設している．**表 2** に鳥取大学のキャンパスネットワークにおけるネットワーク機器の内訳を示す．これらのスイッチの内，284 台の AlaxalA 社製のエッジスイッチにおいて有線 LAN のネットワーク認証を実装した．無線 LAN に関しては，Aruba 社の無線 LAN コントローラである Aruba7210 を用いてネットワーク認証を実装した．

認証サーバとしては，Web 認証を除いて，フリーソフトウェアである FreeRADIUS を用いて構築し，無線 LAN 及び有線 LAN の認証を統合的に扱える様に実装した．利用可能な認証方式としては，PEAP，EAP-TLS のみを受け付け，以前の eduroam JP で許容されていた PEAP でない MS-CHAPv2 の認証は受け付けない様にした．

表 2　鳥取大学におけるネットワーク機器の構成

maker	model	number
AlaxalA	AX8600S08	1
AlaxalA	AX8600S16	1
AlaxalA	AX2230S-24P	61
AlaxalA	AX2530S-08P	28
AlaxalA	AX2530S-24T	85
AlaxalA	AX2530S-24T4X	3
AlaxalA	AX2530S-48P2X	8
AlaxalA	AX2530S-48T	87
AlaxalA	AX2530S-48T2X	8
AlaxalA	AX3650S-20S6XW	5
AlaxalA	AX3650S-48T4XW	1
AlaxalA	AX3830S-32X4QW	1
AlaxalA	AX3830S-44XW	2
AlaxalA	AX260A-08T	8
NEC	IX2215	4
Aruba	Aruba7210	2
Palo Alto	PA-5220	1
Palo Alto	PA-3020	1
Palo Alto	PA-850	1
Cisco	C3560E	1
Cisco	C2960C	3

4　無線 LAN 認証

鳥取大学では，ゲスト用以外の全ての SSID で，既に広く一般的になっている IEEE802.1x を用いた WPA2 の PEAP と EAP-TLS を以前から実装済みである．ゲスト用の SSID では Web 認証を実装しており，Aruba 社の Captive Portal 機能を用いて，認証

ページへのシームレスなリダイレクトを実現している．ゲスト用の SSID のアカウント情報の発行は，専用のシステムを独自に開発し，教職員が複数のゲスト用のアカウントを発行可能としている．

また，前述のとおり，無線 LAN においては SSID の種類は最小限に抑えることが望ましい．そこで，鳥取大学では，2018 年度からは Dynamic VLAN を利用した eduroam への統合を目指し，教育用と研究用の SSID は設定方法を公開しないこととした．また，eduroam JP の認証連携 ID サービスを調査し，なりすましを防げないセキュリティの低い Web 認証に基づいたゲスト用の SSID も廃止を検討している．

5 有線 LAN 認証

鳥取大学では，有線 LAN においては，2017 年度まで講義室などで学生が利用する教育用ネットワークにおいて，ネットワーク認証を全く実装していなかった．そこで，IEEE802.1x 認証と MAC アドレス認証，Web 認証を同時に実装した．新入生以外の全ての在学生や教職員に対して IEEE802.1x の設定変更を強いるのは現実的ではないと考え，経過措置として Web 認証を実装した．また，入学前の利用などを念頭に起き，認証無しでも利用可能とするため，MAC アドレス認証を実装した．本節では，実装したこれらの認証について述べる．

5.1 IEEE802.1x 認証

主に新入生や教職員を対象として，IEEE802.1x 認証を 248 台のエッジスイッチで実装した．エッジスイッチにおいて，新しい端末を検出するための EAP-Request/Identity 送信処理を抑止し，端末からの任意のフレームを受信した際に個別に EAP-Request/Identity を送信し，認証処理を実施する設定とした．

クライアントの設定に関しては，Windows 10 1709 (2017 年の fall creator update) によって有線 LAN での IEEE802.1x 認証がデフォルトで有効化された．これに伴い，有線 LAN での IEEE802.1x 認証のサービスを起動する設定が不要となり，設定がある程度軽減された．しかしながら，無線 LAN の場合と同様，より安全な設定のためには RADIUS サーバの設定が難しい．

5.2 MAC アドレス認証

新入生への必携 PC の説明会などのために，アカウント情報を有していなくても，ネットワークに接続可能とする講義室が必要となる場合がある．また，IEEE802.1x 認証に対応していないプリンタなどの機器もネットワーク接続可能とする必要があるが，もちろんこれらの機器では Web 認証はできない．

上記の様な場合に対応するため，MAC アドレス認証も導入した．FreeRADIUS の files モジュールを利用し，Calling-Station-ID がユーザ ID となるファイルを別途作成した．また，機器の判別を用意にするため，ホスト名が存在している機器に関しては，ホスト名を登録可能とした．同様のモジュールを用いて，セキュリティインシデント時などに通信を遮断可能とするために，ブラックリストとして MAC アドレスを登録可能とした．

5.3 Web 認証

IEEE802.1x 認証のためには新規の難しい設定が必要となる．新入生に対しては全学共通科目である情報リテラシ教育の講義内で対応することで周知できると思われる．一方，新入生以外の全ての在学生や教職員に対して，ある年度から IEEE802.1x 認証を強いるのは現実的ではないと思われた．そこで，マニュアルや事前知識がなくとも直感的に操作可能であろうと思われる Web 認証を経過措置として有効化した．Web 認証には，鳥取大学の統一認証として採用している Shibboleth を利用した．Web 認証のための Shibboleth SP を構築し，認証していない端末をネットワークに接続する際には，Shibboleth IdP の画面へとリダイレクトされる様にした．しかし，Web 認証だけを実装した場合認証が完了するのに時間を要したり，SSL/TLS のページの表示ができないという問題が発生した．そこで，次節に示す様に Captive Portal を実装した．また，従来の HTTP や SSL/TLS 通信を横取りしてリダイレクトする処理がスイッチに負荷をかけることが判明したため，スイッチにてリダイレクトしない様に設定を変更した．

6 Captive Portal の実装

前述のとおり，Web 認証には認証が完了するのに時間を要したり，SSL/TLS のページが表示できないという問題がある．それを解決する 1 つの手段として，Captive Portal を実装し，OS に Captive Portal を検出させることが挙げられる．各 OS は，Captive Portal の存在を独自の方法によって検出する．そして，Captive Portal が存在した場合には Captive Portal のページを表示する．Captive Portal を検出することによって，OS が Windows Update などの不要な通信を発生させることなく，また，HTTP や SSL/TLS

の通信を横取りしたリダイレクトも不要となり，認証ページへのシームレスな誘導が可能となる．

そこで，鳥取大学内において Captive Portal を実装した．Captive Portal の実装にあたっては，各 OS が Captive Portal を検出するためにアクセスする URL が Shibboleth SP へのアクセスとなる様にした．具体的には，URL に含まれる FQDN の NS レコードを学内の DNS サーバに向け，学内の DNS サーバで FQDN に対する A レコードを Shibboleth SP の IP アドレスになる様にした．この様にすることで，各 OS が自律的に Shibboleth SP にアクセスする様にでき，前述の問題が解決できた．

しかし，特定の環境で Captive Portal 検出が有効になっていない OS もある．Windows OS においては有線 LAN 及び無線 LAN の両方で Captive Portal 検出機能がデフォルトで有効になっている．一方で，macOS では無線 LAN だけでデフォルトで有効になっており，有線 LAN で有効にするには特別な設定が必要となる．そのため，macOS では有線 LAN においては，Web 認証によって認証を実現するのは難しいと考えられる．しかし，macOS では IEEE802.1x 認証が比較的容易に設定できるため，macOS の利用者には IEEE802.1x 認証を推奨することとした．

なお, RFC7710 [2] により規定された DHCP や RA のオプションによる Captive Portal Detection への対応を試みた．しかし，Windows OS，macOS 共に端末が当該の DHCP オプションを送信してきおらず，2018 年 9 月現在では実装されていないと考えられる．

7 IEEE802.1x 自動化スクリプト

IEEE802.1x 認証では, 安全のために RADIUS サーバの設定まで実施する場合，かなり設定が煩雑になってしまう．そのため，ある程度設定を自動化できると利用者にとって便利であると考えられる．無線 LAN に関しては，eduroam CAT [3] と呼ばれる取り組みがあり，各 OS に対応したアプリケーションが配布されている．しかし，無線 LAN における設定のみしか行えず，有線 LAN の設定には対応していない．

そこで，現在，無線 LAN 及び有線 LAN の IEEE802.1x 認証の設定を自動化するツールを作成中である．作成にあたっては，OS の変更に柔軟に対応するため，スクリプト言語での実装を進めている．利用者は自身のユーザ名とパスワードを入力するだけで，設定が完了するものを目指している．

8 おわりに

本稿では，鳥取大学におけるネットワーク認証の取り組みについて述べ，得られた知見を報告した．

参考文献

[1] Apple Inc. iOS および macOS で 802.1X 認証の証明書信頼を設定する． https://support.apple.com/ja-jp/HT207866.

[2] Warren "Ace" Kumari, lafur Gumundsson, Paul Ebersman, and Steve Sheng. Captive-Portal Identification Using DHCP or Router Advertisements (RAs). RFC 7710, December 2015.

[3] GEANT. eduroam CAT. https://cat.eduroam.org/.