

eduroam の認証要求の集中による過負荷事象の発生と対策実施について

山崎 國弘^{1), 2)}, 磯部 千裕²⁾, 永田 正樹¹⁾

1) 静岡大学 情報基盤センター

2) 株式会社 アバンセシステム

yamazaki.kunihiro@shizuoka.ac.jp, c-isobe@avancesys.co.jp,
nagata.masaki@shizuoka.ac.jp

Occurrence of overload events due to concentration of eduroam certification requests and implementation of countermeasures

Yamazaki kunihiro^{1), 2)}, Isobe Chihiro²⁾, Nagata Masaki¹⁾

1) Center for Information Infrastructure, Shizuoka University.

2) AvanceSystem Corporation.

概要

静岡大学では 2018 年 3 月より 300 台以上のアクセスポイントで eduroam が利用できるようにした。学内ネットワークの混雑低減を目的に、インターネット接続のみの通信は eduroam 利用を推奨している。eduroam の利用拡大で特定の時間帯に無線 LAN 接続が不安定になる事象が発生し、認証要求の集中が原因と判明したため認証サーバの負荷軽減対策を実施し改善効果を確認することができた。本稿では大学における無線 LAN 接続の認証要求に特有の日変化、認証要求の輻輳状態が発生したときの利用者への影響、LDAP (Lightweight Directory Access Protocol) への適切なインデックス有無による性能の違いなどについて報告する。

1 はじめに

2018 年 3 月の eduroam サービス開始から順調に利用が拡大し、2019 年 7 月には 1 日の eduroam 接続ユーザ数が約 2,900 ユーザ、月間の接続端末数は 6,000 端末となり無線 LAN 接続全体の 35% を占めるようになった。同じく 2019 年 7 月の平均で eduroam を利用し他大学から静岡大学アカウントで接続するユーザが一日当たり 30 ユーザ、静岡大学キャンパス内から他大学のアカウントで接続しているユーザが一日当たり 15 ユーザ、ゲスト用アカウントを利用するユーザが一日当たり 15 ユーザと前年と比較して 2 倍に利用が拡大している。

eduroam IdP (Identity Provider) サーバは zabbix[1] で監視しており、eduroam の利用拡大により eduroam IdP サーバの CPU 使用率が 90% 以上となるアラートが 2019 年度から頻繁に発生するようになった。授業開始時に無線 LAN 接続が不安定になる事があったという報告も寄せられている。これらの事象の原因を調査したところ、短時間に非

常に多くの認証要求が発生し輻輳状態になっていることが確認できた。また、認証処理時の LDAP 検索において、適切なインデックスが設定されていないことが確認できた。それらが原因となり、認証処理時に仮想サーバが高負荷状態となっていることが判明したが、原因調査と対策実施の過程でいくつかの知見を得ることができた。

2 静岡大学の eduroam 無線 LAN 環境

2.1 利用状況

本学では無線 LAN アクセスポイントのマルチ SSID (Service Set Identifier) 機能を使用し学内ネットワーク接続と eduroam の 2 種類の無線 LAN サービスを提供している。eduroam は概ね学部単位で光ケーブルによる商用インターネット接続サービスを導入し、インターネット接続のみのトラヒックがキャンパススイッチ (静岡、浜松キャンパスの最上位スイッチ)、データセンターのコアスイッチやネットワークセキュリティ機器を通過しないようにして学内ネットワークの混雑低減を図つ

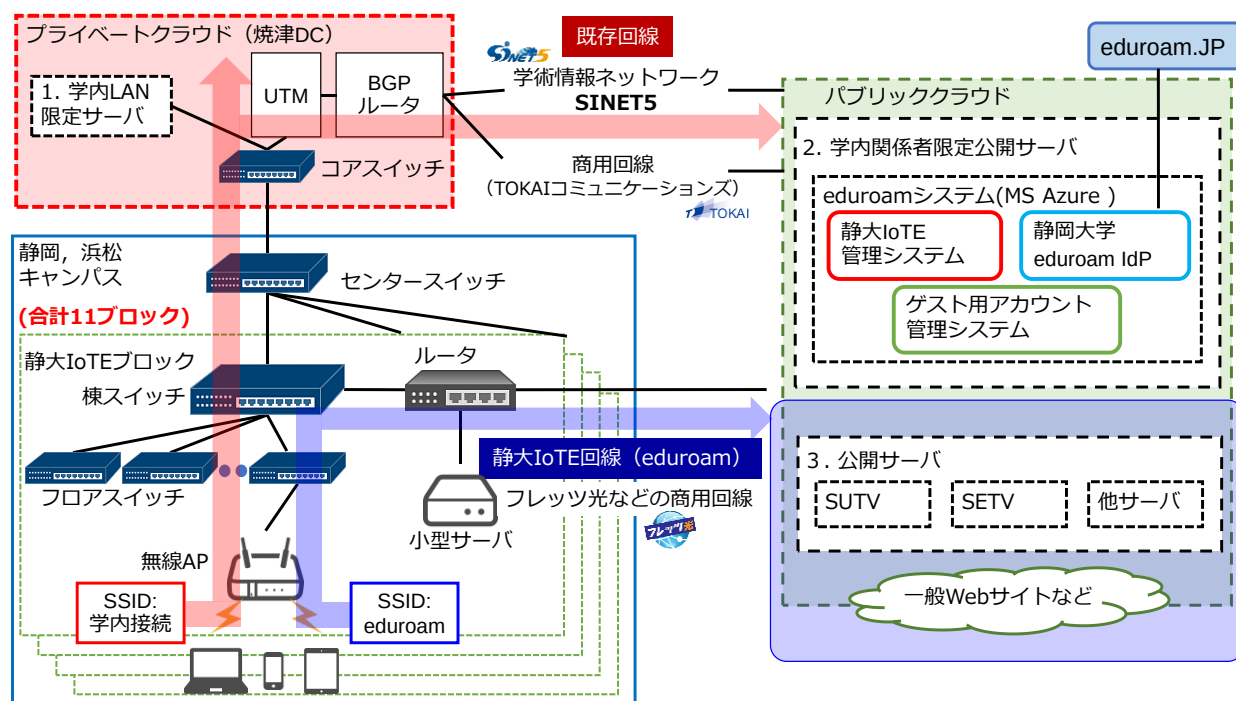


図-1. 静大 IoTE 概要

表-1. eduroam IdP システム概要

eduroam IdP	
Azure Virtual Machines	D2 v3
OS	CentOS 7.4
アプリケーション	samba 4.6.2
	FreeRADIUS 3.0.13-8
	openldap-2.4.44
	openssl-1.0.2k-8

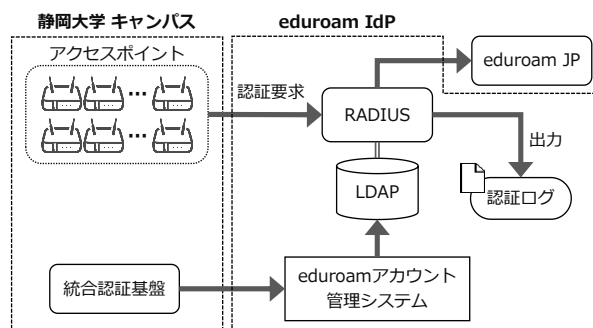


図-2. eduroam IdP システム構成図

ている [2] .

eduroam は VLAN で学内ネットワークから完全に独立したネットワーク構成とし、万一無線 LAN 接続した端末の不適切な利用による問題が発生した場合でも、その影響がキャンパス全体に波及しないようにしている。本学ではこの eduroam 無線 LAN システムを静大 IoTE と呼んでいる。図 1 にシステムの全体構成を示す。

2.2 eduroam IdP の構成

eduroam に端末を接続するための認証処理はパブリッククラウドに設置した eduroam IdP で実施している。大規模災害等でデータセンターに設置した本学の認証基盤と接続ができない場合でも、他大学から静岡大学のアカウントで eduroam の利用が継続できるよう認証情報を eduroam IdP に配置している。eduroam IdP はオープンソースの RADIUS (Remote Authentication Dial In User Service) と LDAP で実現している。表-1 にシステム環境を、図-2 に eduroam IdP のシステム構成を示す。

3 認証負荷と過負荷事象

図-3 に eduroam IdP サーバにおける 2019 年 4 月 24 日 8 時から 17 時までの CPU 使用率の変化を示す。授業の前後に CPU 使用率の急増が見られ、1・2 時限目と 3・4 時限目の間は 100% の状態が継続している。この CPU 使用率の変化は授業のある日に共通して見られる。

この時間帯を含む 10 時 00 分から 59 分の CPU 使用率と eduroam IdP への認証要求数の関係を図-4 に示す。単位時間当たりの認証要求が増加している場合は CPU 使用率の上昇は抑えられ、CPU 使用率が 100% の状態になると認証要求が減少しても CPU 使用率がなかなか減少しないヒステリシス曲線になっていることが確認できる。無線 LAN 管理サーバ[3]の認証処理、RADIUS の認証要求、LDAP の認証要求は同様

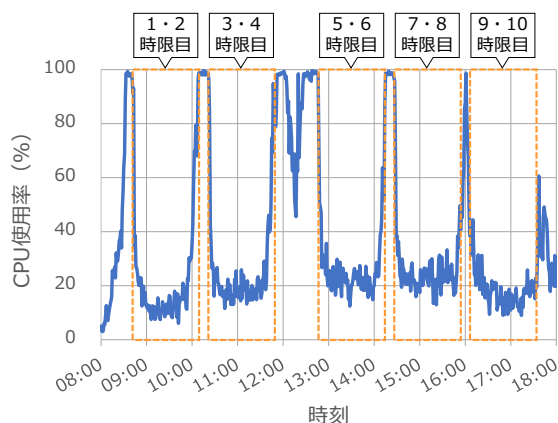


図-3. 仮想サーバの CPU 利用率 日変化

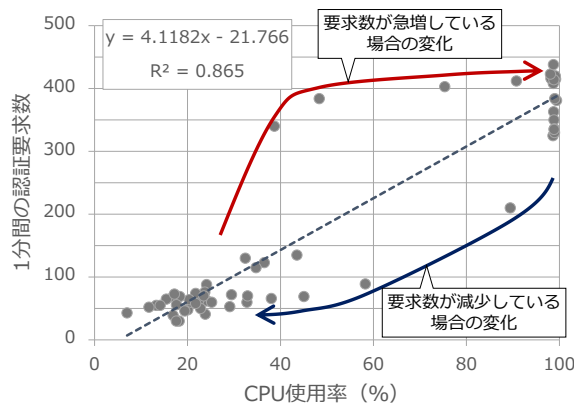


図-4. CPU 使用率と認証要求の関係

の変化を示していることから短時間に認証要求が集中したことで処理しきれない認証要求が累積する状態になっていたと考えられる。無線 LAN 接続の認証処理が著しく遅れると端末は無線 LAN 接続処理を繰返し実行する可能性がある。これにより認証要求が更に増加する輻輳状態が発生していたと考えられる。また、授業開始時に無線 LAN 接続が不安定になる事があったという報告とも一致している。

本学の環境では毎分 200 件程度の認証要求までは正常に動作しているが、実際にはその 2 倍以上の認証要求の発生が見られた。

4 対策実施と効果確認

eduroam IdP の処理能力向上のために LDAP に対し適切なインデックスを追加することとした。LDAP へのインデックス追加にあたっては、稼動している現行システムと同一環境の検証用システムをパブリッククラウドに構築し、認証要求を発生できる試験ツールを用いて、事象の再現、インデックス追加後の CPU 使用率低減効果比較による適切なインデックスの検討、ゲスト用アカウン

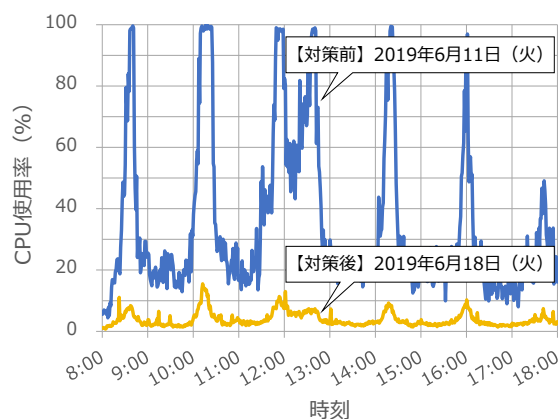


図-5. 対策前後の CPU 使用率の比較

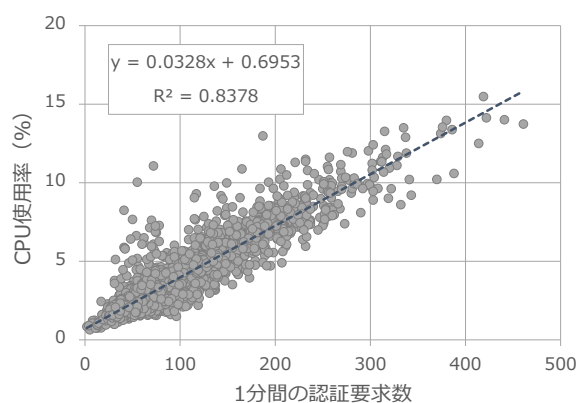


図-6. CPU 使用率と 1 分間の認証要求数

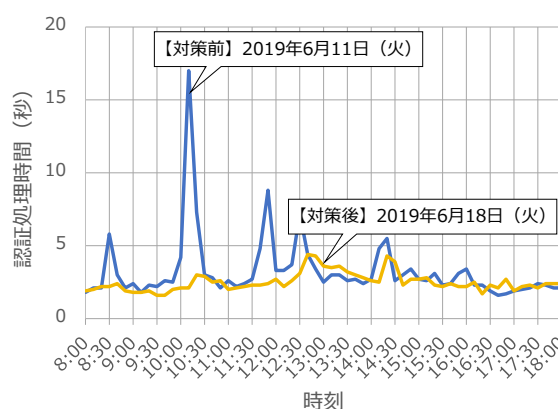


図-7. 対策前後の認証処理時間の比較

ト発行処理時間が遅延しないことの確認などの検証を実施した。その上で、本番システムの LDAP へインデックス追加を行った。

図-5 に対策前後の CPU 使用率変化の比較を示す。無線 LAN 利用は特に火曜日が多いため、対策前は 6 月 11 日、対策後は 6 月 18 日を比較している。対策後も授業時間の前後に CPU 使用率の上昇が見られるものの、ピークは 15%程度の小さな値になっている。対策前後の平日 1 週間の平均を比較すると最大値では 87%の低減と大きな効果があったことが確認できた。図-6 に対策後の CPU 使用率と 1 分毎の認証要求数の関係を示す。6 月 14 日

から6月20日の内の平日5日間における、8時00分から17時59分のデータを使用している。LDAPへの適切なインデックス追加により認証要求に対するeduroam IdPの処理能力は12倍に拡大したことが確認できる。また、現在のシステム構成のままでCPU使用率80%程度の負荷時には、2,400件／分の認証要求の処理が可能であると推測される。図-7に対策前後の認証処理時間変化の比較を示す。図-5と同じく対策前は6月11日、対策後は6月18日を比較している。認証処理時間は無線LAN管理サーバのログから、端末がアクセスポイントに接続した時間から接続承認のイベントが記録されるまでの時間を秒単位で計算している。eduroam IdPの認証処理以外にアクセスポイントの処理時間も含まれている。10分間にeduroamに接続した端末毎の時間を計算し、その平均値を算出した。対策前の6月11日はCPU使用率100%が10分以上継続した10時20分頃に極めて大きな遅延が発生しているが、対策後の6月18日は極端な遅延は発生していない。

5 おわりに

eduroam IdPにおける単位時間当たりの認証要求の集中による仮想サーバの過負荷状態の調査及びその対策実施で以下の知見を得ることができた。

1. パブリッククラウドを使用したシステム運用の効果

4項で述べたように稼働中のシステムと同じ構成の検証システムを構築し、事象の再現、対策の効果確認、関連機能への影響発生有無の確認などを、コストを抑えて実施することができた。運用開始後の負荷状況が把握できない新規サービスや利用拡大で負荷が大きく増加することが予想されるサービスでは特に有効だと考えられる。

2. 大学における無線LAN特有の負荷の変化

学生が授業スケジュールに従い教室、図書館、福利厚生施設などを移動するため、授業の前後に非常に大量の認証要求が発生することがわかった。無線LANアクセスポイントの整備が進み利用が拡大するほどこれらのパターンも顕著になると考えられる。無線LANがネットワーク接続の基本サービスになり利用者が複数の端末を同時に接続する、新しい端末デバイスが利用されるなど今後も変化が予想される。無線LANの利用状況及び構成する機能の負荷状況などを継続的に監視・分析できる仕組みの確立が重要になると考えられる。

3. eduroam IdPが輻輳状態になったときの影響

無線LANは端末が自律で動作する部分が大きく、認証処理つまり端末接続処理時間に遅延が発生すると再接続による輻輳状態になりやすく、利用者は無線LANの接続が不安定になったと感じることがある。

これらのことから無線LAN利用者の満足度向上のためには、無線LANアクセスポイントの性能だけでなく認証機能などの無線LAN関連システムの性能とバランスが取れていることが重要である。また大学特有の無線LAN利用パターンに対応し大きく変動する負荷に対して妥当な性能のシステムを構築するには、負荷状況の継続的な測定が必要であることが確認できた。

eduroamと同一設備で運用している学内ネットワーク接続用の無線LANも、eduroamと同様の利用傾向を示していると考えられる。今後は学内ネットワーク接続用の無線LANについても同様の分析を行いたいと考えている。

参考文献

- [1] zabbix
<https://www.zabbix.com/jp/features>
- [2] 永田正樹, 磯部千裕, 安原裕子, 古畑智博, 高田重利, 松村宣顕, 山崎國弘, 長谷川孝博, 井上春樹, ”パブリッククラウドとオープンソースソフトウェアを用いたトラフィック分散型eduroam基盤「静大IoTE」の構築”, 学術情報処理研究 No. 22, 2018年9月.
- [3] 無線ネットワーク管理システム UNIFAS
<http://www.furunsystems.co.jp/product/detail/unifas.html>