信州大学認証ネットワーク「セキュアネット 2010」における認証スイッチの拡張と整備

Expansion of the Authentication Switch for Shinshu University User Authentication Network System “Secure-Net 2010”

鈴木　彦文†，永井　一弥†，浅川　圭史†，今井　美香†，不破　泰†
Hikofumi SUZUKI†, Kazuya NAGAI†, Yoshifumi ASAKAWA†,
Mika IMAI†, Yasushi FUWA†

h-suzuki @shinshu-u.ac.jp, kznagai @shinshu-u.ac.jp, asakawa @shinshu-u.ac.jp,
mika_imai @shinshu-u.ac.jp, fuwa@shinshu-u.ac.jp

†信州大学総合情報センター
† Shinshu University Integrated Intelligence Center

概要

信州大学では平成 12 年より光回線を用いた Gigabit Ethernet ネットワークを構築してきた. そして 2004 年に本学全域に対してユーザ認証可能な認証ネットワークシステムとして「信州大学セキュアネット 2004」を構築した．本ネットワークシステムは Private IP Address と NAT をベースとし，Web 認証システム，統合認証システム，ポータルサイトと連動する認証ネットワークシステムである．その後，マルウェア，P2P 対応，不正なアクセスを行ったユーザの特定，ネットワークの利用を前提とした学生ノート PC 購入など，認証ネットワークに対する大幅な機能追加と性能向上が要望された．これらに対応するため新認証ネットワークシステムとして「セキュアネット 2010」を構築し 2010 年 4 月より運用を開始した．本ネットワークシステムにより，安全性の高い認証ネットワークを大規模化させるだけでなく，本学におけるセキュリティ上の対応や，ユーザ個々の追跡など高度な分析や制御が可能となった．しかしながら，一部において大量のユーザが同時に認証ネットワークへ接続し認証を行った場合に障害が発生した．これに対応するための方法を述べる．

キーワード

認証ネットワーク，セキュリティ，ユーザ挙動監視，ネットワーク構築運用管理

1. はじめに

信州大学は全学で利用可能な認証ネットワークとして「セキュアネット 2004」を構築し運用してきた．「セキュアネット 2004」では Class B 程度のネットワークに関してゲート認証を行ってきた．しかしながら，認証ネットワークに対し，多くの機能拡張や性能向上の必要性が高まってきた[1].

更に，本学においては学内外合わせて公式な拠点だけでも 43 拠点(2011 年 7 月現在)を有する遠隔講義・会議

システム SUNS(Shinshu Ubiquitous-NetSystem)を運用している[2,3]．従来であれば遠隔講義・会議システムは認証ネットワーク内に設置することはなかったが，現在では安全性の確保のために認証ネットワーク内への設置が進んでいる．遠隔講義・会議においては定常的にネットワークの帯域を必要とする上，安定している必要がある．また，本学はほぼ全ての学生にノート PC の購入を促しており，授業や実験実習においても活用されている．そして授業においては認証ネットワークより本学 e-Leaning システムである eALPS [4,5]が参照される．

このよう認証ネットワークの安定運用は，授業や実験実習を実施するにあたりおいて欠くことのできない要素となっている．これは教育の質的保証においても重要であり，安定性の高いネットワークを設計，構築し運用することは業務として責任を持って遂行しなければならない．

このような要望を満たすネットワークとして信州大学では「セキュアネット 2010」を構築した．「セキュアネット 2010」では，Class A 規模の Private IP Address ネットワークを構築しつつ，更に Class B の Global IP Address も包含するトータルな認証ネットワークとして構築された．更に 2010 年度より「高速高信頼性ネットワーク」(3 年計画)構築に伴い，初年度信州大学主要 5 キャンパス(松本，長野(工学)，長野(教育)，上田，南箕輪)の全てのキャンパス内建物間光回線の整備とキャンパス間ネットワーク整備を実施した．2 年目以降の計画において，「セキュアネット 2010」全ての建物にて利用可能とするため拡充を行っている．

本稿では「セキュアネット 2010」の運用と拡充において発生した問題とその解決方法として実施した認証スイッチの拡張と整備について報告する．

2. 信州大学ネットワークと認証ネットワーク「セキュアネット 2010」

信州大学は松本，長野(工学)，長野(教育)，上田，南箕輪の主要 5 つのキャンパスからなる大学であり，各キャンパス間は 1C/8C の光回線(SM 9.5/125 μm)にて接続されている(図 1)[6]．また 2010 年度より「高速高信頼性ネットワーク」の構築を開始し，信州大学ネットワークのリプレースを実施している．認証ネットワークである「セキュアネット 2010」は総合情報センターにおける「教育用計算機システム」の一部として 2010 年度から運用を開始し，更に「高速高信頼性ネットワーク」の構築において認証機能を全ての建物に対し拡充する(前者にて 60%程度の建物に供給したので，後者にて 100%へ拡充する)．

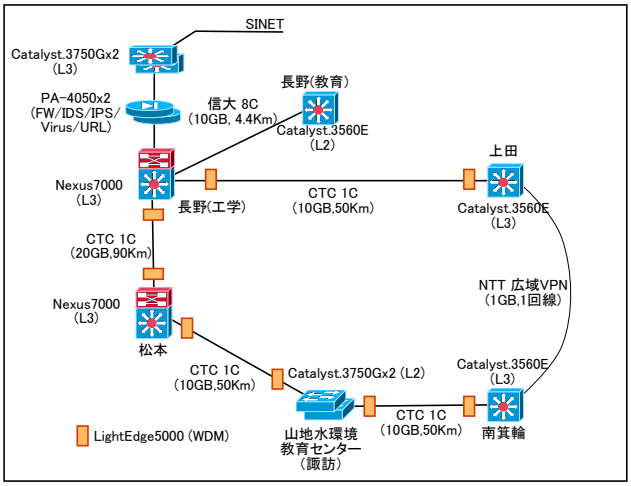

図 1 信州大学キャンパス間ネットワーク構成概要

図 1 に示す信州大学キャンパス間ネットワークにおいて，「セキュアネット 2010」構築における基本コンセプトは次に示す通りである[1].

1. 信州大学全域に対する広域サービス
2. 広域化に伴う性能の低下最小限化
3. 導入，運用コストの低減
4. DHCP サービスと適切な割当対処
5. Web/MAC 認証の実施と柔軟なポリシー適用
6. 信大ポータルサイトや各種サーバと連携
7. UTM(Unified Threat Management) との連携
8. IP Address/MAC Address/ユーザ単位でのトラフィック制御と統計情報の取得
9. P2P アプリケーションやゲーム，マルウェア等の挙動監視と制御
10. 長期不使用 IP Address の洗い出し

上記ポリシーに基づき構築した認証ネットワーク「セキュアネット 2010」の概要は図 2 となる．本認証ネットワークの最大のポイントは，L2 認証とゲート認証(Captive Portal 認証)，及び，ポータルサイト認証を同時に行うことにより，ユーザからはポータルサイトにログインする動作だけで全ての認証が完了している認証ネットワークである点である．これにより上記 1.～10.目標達成が可能となった．

3. 「セキュアネット 2010」の問題と課題

「セキュアネット 2010」の運用を実施した 2010 年度において，運用から問題や課題が発生した．詳細は参考文献[1]に示すが，とりまとめると次のようになる．

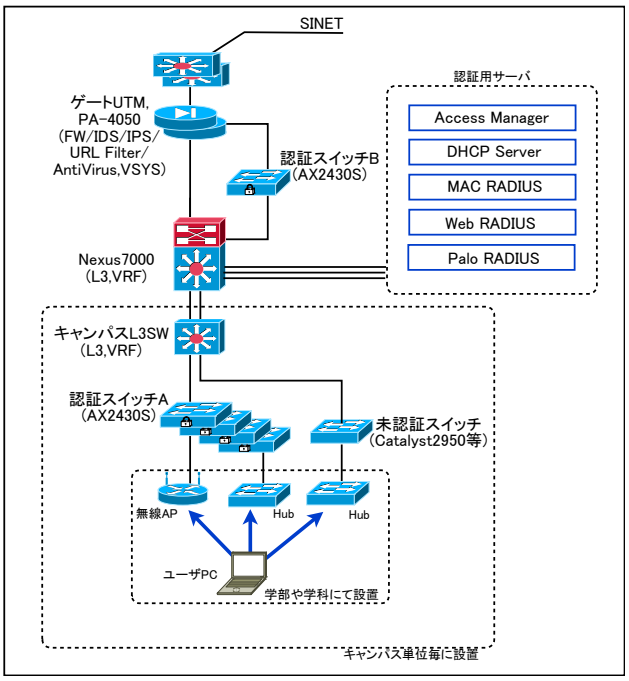

図 2 セキュアネット 2010 ネットワーク構成概要

1. Global IP Address のネットワークへの適用とポリシーの拡大

現在は Private IP Address ネットワークのみに認証を適用しているが，今後は Global IP Address ネットワークにも適用する．

2. 同時 login 性能の向上

600 人が同時に login した場合，全てのユーザにおいて 10 秒以内に処理を完了する．

3. 認証連動部分の改善

認証スイッチや UTM (PA-4050) では，最終的にバックエンドにある Web/Palo RADIUS に認証情報をエントリする必要がある．現在，このエントリ情報の共有は https にてユーザ PC と認証が必要(エントリ情報が必要)な装置間で逐次的に交換しているが，バックエンド内で閉じて共有する仕組みを構築する．

4. 非正規に設置された NAT や DHCP サーバ機能を持つ機器への対応

セキュアネットに限らずネットワークを運用する上で発生する重要な障害の 1 つとして，非正規に設置された NAT 機器と DHCP サーバがある．これを検出する仕組みを構築することにより，授業実験を安定して開催できる．

5. ユーザへの情報提供

希望するユーザ対し，当該ユーザ ID の情報をベースとしたトラフィックの状況等をユーザ単位で供給する．こともできるため，例えばマルウェアの挙動等を個々人でも確認することができる．

6. メーカーへの要望

UTM 機器の Palo Alto Networks 社製 PA-4050 において，ユーザ認証機構である Captive Portal が http でしかできない．これにより認証フローが複雑化しているため改善を要望している．また，認証スイッチの ALAXALA Networks 社製 AX-2430 において，認証待ちにおける処理が滞留する状況の改善を要望している．

本稿では上記の問題や課題から特に 2.同時 login 性能の向上に関して，設計と取り組みについて述べる．

4. 「セキュアネット 2010」における同時 login 性能向上計画と設計

前章にて提示した同時 login 性能において，最も性能的にボトルネックとされたのは，ゲートに設置されている UTM による Captive Portal 認証やポータルサイトではなく，L2 認証スイッチにおける同時認証性能である．今回投入した AX2430 シリーズでは，L2 認証における同時認証処理能力が実効で 40 以下である．また，本スイッチにはそれ以外の問題点として，不要に認証待ちとなった場合のセッション切断までの時間が長い等，認証処理そのものに関する問題があったが，これらは適宜ファームウェアが改善されてきた．しかし，同時処理等基本性能に関わる部分についてはファームウェアの改善では対処できない．

このような根本的なボトルネックの問題を解消するため，L2 認証スイッチの構成を変更することで大量の同時 login が発生しても耐えうる構成を考案した（図 3）．

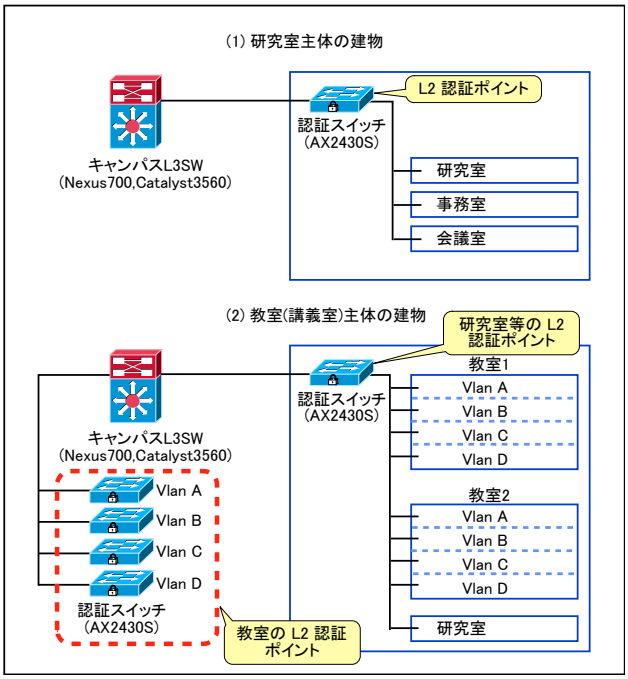

図 3 認証スイッチの設置形態と認証ポイント
(1)研究室主体の建物の認証と，(2)教室(講義室)主体の建物への L2 認証スイッチの設置と認証ポイント

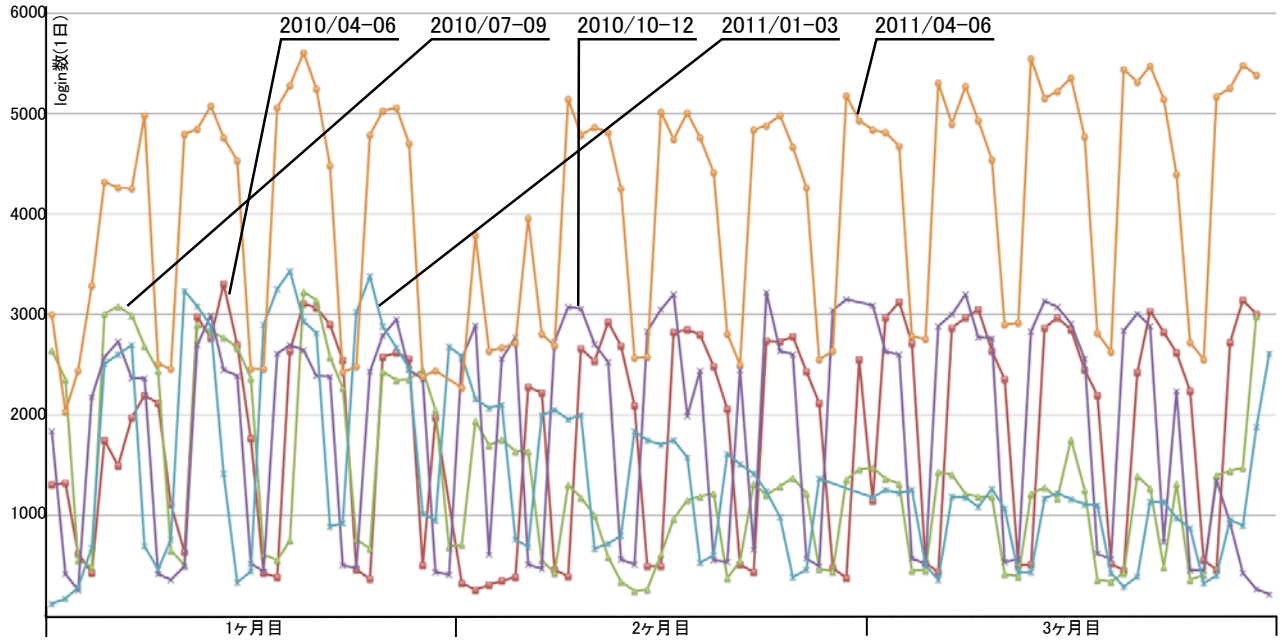

図 4 「セキュアネット 2010」 認証数(login 数)の推移 (四半期ごと 2010/04 ～ 2011/06)

図 2 の(1)は通常の研究室主体の建物に対する L2 認証を表している．研究室主体の建物の場合，認証スイッチは建物に 1 台設置され，同一建物内の L2 認証をすべて実施する．この場合，認証ネットワークに同時に多数のユーザが login することは稀であり，AX2430 の同時認証処理が 40 セッションであることは問題にならない．

問題は教室や講義室主体の建物の場合である．特に 1 年生向けの授業では，学部等で指定されたノート PC(持ち込み PC)を利用した場合，画面を説明しながら 1 ステップずつ授業が開催される．また，生協主催の購入 PC 説明会等でも 300 台近いノート PC の基本的な操作説明が，やはり画面を説明しながら 1 ステップずつ説明される．この場合，40 台以上のノート PC が同時認証する事態が発生し，L2 認証が困難となった．2010 年の 4～5 月において頻繁に発生した障害の多くは L2 認証スイッチのこの問題によるものが少なくなかった．

そこで教室や講義室主体の建物に対応すべく，図 2 (2) のような接続方法を考案した．図 2 (2) の例では教室 1,2 を 4 エリアに区切り，それぞれに Vlan を設定する(1 つの VLan あたり 20～30 人の学生がノート PC を接続すると想定)．そしてその Vlan 毎に認証するスイッチをキャンパスセンタースイッチ側に設置し，L2 認証機能のみを提供するのである．ボトルネックを解消するための重要な点は，同時に認証が発生した場合に分散させることである．つまり，教室 1 や 2 において認証ネットワークを利用する授業があったとしても，全く同じタイミングで認証が同時にかからない限り本構成で問題ない．これは教室の数が多くなれば異なる教室で同時に認証が発生する可能性が高まるが，現在の運用においては，松本キャンパス(7600 人)では 8 台，長野(工学)キャンパス(2700 人)では 6 台の AX2430 を認証分散のために設置されている．

5. 認証ネットワークのトラフィックデータと運用状況

前章で述べた設計を実施したのは 2010 年 10 月からである．また，図 4 は「セキュアネット 2010」における login 数を四半期毎にまとめたものである．2010 年度においてはピークでも 3000 login であり，特に 2010 年 9 月までは授業の方法によっては同時認証の問題が発生していたが，前章の対策が完了して以降，「セキュアネット 2010」における同時 login 時における L2 認証の問題は発生していない．特に図 4 では 2011 年度に入り最大 login 数のピークが 6000 login 近くまで増加した．それにも関わらず，認証関係の障害に関しては L2 認証においても，Captive Portal 認証においても，またポータルサイトの認証においてもほぼ発生していない．

図 5 は「セキュアネット 2010」における 2010 年度の総認証回数(login 数)を時間にて集計したグラフである．昨年度のピークは 9～16 時であるが，これは主に学部学生が利用する時間であり，認証ネットワークの拡充と共に認証数やピーク時間が変動する可能性がある．

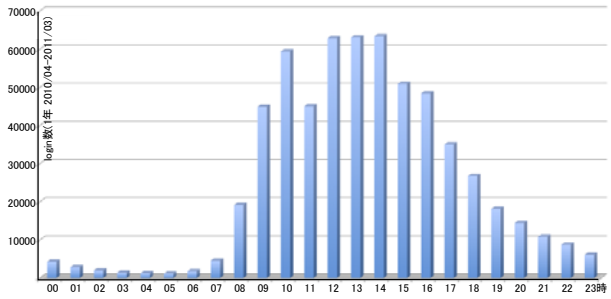

図 5「セキュアネット 2010」年間認証数(login 数)
2010/04 – 2011/03

6. 結果と今後の課題

教室(講義室)主体の建物に関して，認証スイッチをキャンパスセンタースイッチにまとめて収容し，教室を Vlan で分割し対応する認証スイッチにて認証させる方法で同時認証の問題が解決した．認証のピークが倍増した(図 4)今年度において, 本対策が完了していたため認証に関わるトラブルは発生していない．更に授業において同時に login 操作をさせる授業の担当教員(特に昨年度障害が発生した授業を中心)に，今年度の障害状況に関する問い合わせを実施したところ，授業の進行には全く問題がなかったとの回答を得たことから，本対策が非常に有効であったと考えられる．

また，通常の設計であれば，教室にて同時認証の問題が発生した場合，教室側に大量の認証スイッチを設置することとなるが，センタースイッチ側に認証スイッチをまとめる本対策は費用対効果や HA の面でも非常に優れており有効な対策であると考えられる．

7. まとめ

本稿では大学として必要性が高まってきた認証ネットワーク「セキュアネット 2010」の同時認証における障害対策として認証ネットワークを有効に拡張するための設計を行い構築した経緯をとりまとめた．

認証ネットワークは安全性や管理者に取っての利便性だけを考慮するのではなく，利用者の利便性の向上が重要であると考えている．教職員が授業の運営で工夫しなくとも，ストレス無くあたりまえのように利用できるシステムとして, 今後も「セキュアネット 2010」を拡充させる予定である．

更に，「セキュアネット 2010」は今後の認証ネットワークの拡充を見据え，更に完成度を高めるために 600 人同時 login を 10 秒以内に達成する目標を 2011 年 9 月までに達成する予定である．

謝辞

「セキュアネット 2010」の設計や構築，及び，本稿にて提示している認証やトラフィックのデータ解析に関して，ネットワンシステムズ株式会社に支援をいただきました．ここに感謝の意を表します．

参考文献

[1] 鈴木彦文,永井一弥,浅川圭史,今井美香,不破泰:UTM を用いたユーザ認証ネットワーク「セキュアネット 2010」の構築;学術情報処理研究,No.14,pp.21-30,2010

[2] 森下孟,茅野基,鈴木彦文,永井一弥,新村正明,矢部正之:高等教育コンソーシアム信州における大学間遠隔講義システムを活用した遠隔講義「K3 茶論」の実践;学術情報処理研究,No.14,pp.105-116,2010

[3] 森下孟, 新村正明, 茅野基, 鈴木彦文, 永井一弥, 矢部正之, “大学間遠隔講義システムの構築と試行”，日本教育工学会，第 25 回全国大会, P1p-FLS-17, Sep. 2009.

[4] 五月女雄一,鈴木彦文, 新村正明, “複数の教育支援システムの相互利用とシステム間の情報共有を実現する教育基盤システムの構築と運用”,教育システム情報学会研究報告, 23, (7), pp.118-123, Mar. 2009.

[5] 五月女雄一, 鈴木彦文, 新村正明, “教育支援システムの疎結合で構成される教育基盤システム「eALPS2.0」”,情報処理学会研究グループ報告, 第10回 CMS 研究発表会, pp.1-4, Dec. 2008.

[6] 山崎洋一，“ネット構築の現場から”，日経 NETWORK, 2010 年 7 月号(第 123 号), pp.56-59.