ISSN 1341-139X

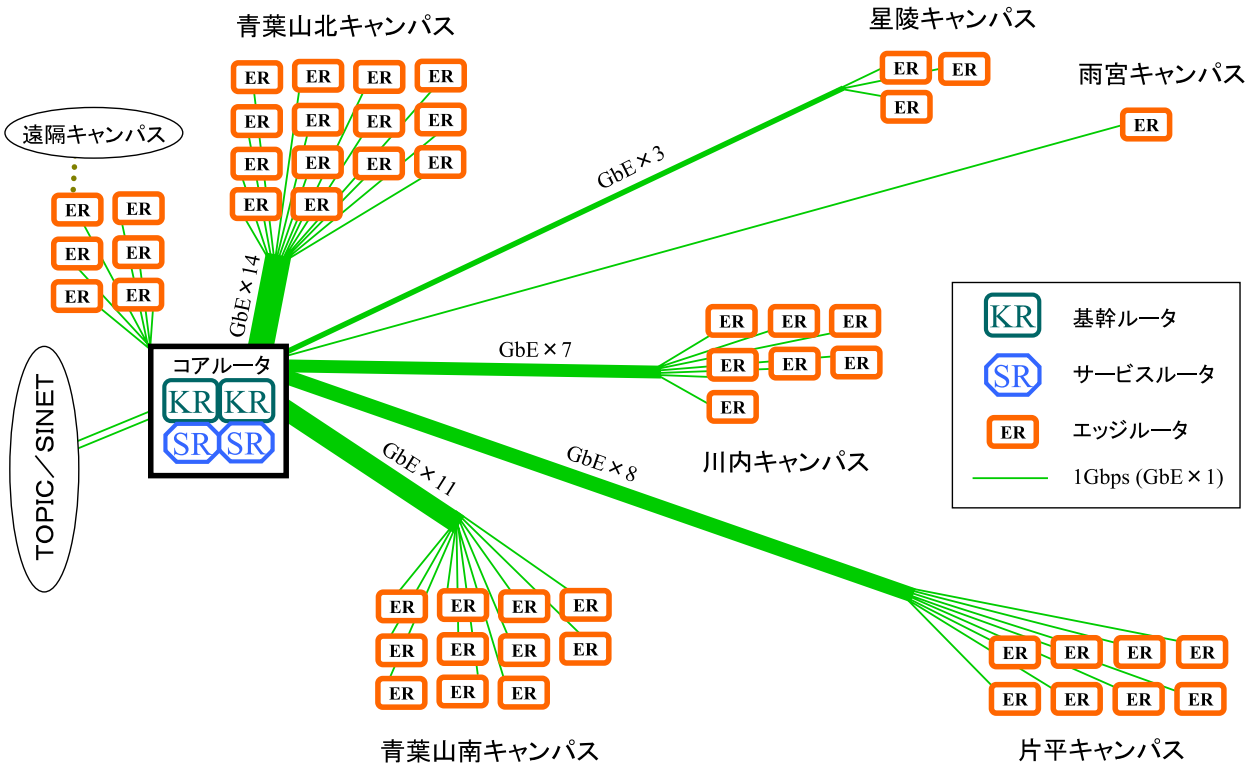
サイバーサイエンスセンター
情報部情報基盤課

東北大学情報シナジー機構

TAINSニュース

東北大学情報シナジー機構 情報シナジー広報室 TAINS ニュース編集グループ

2008.12.25 No.36



次世代 TAINS の基幹ネットワーク構成

目 次

お知らせ 2
情報シナジー機構の改編について ..... 鈴木陽一 3
次世代 TAINS の概要紹介 ..... 水木敬明, 曽根秀昭 5
全学的な統合認証システムの実現に向けて ..... 木下哲男, 早川美徳 14
学内ローミングおよび国際ローミングに対応した情報科学研究科・新無線 LAN システムの構築について ..... 後藤英昭 17
編集後記 23

※ TAINS ニュースは，全教員および各研究室と事務等の各室に 1 部ずつ配布しています。職員・学生の皆さんにもご回覧ください。また，WWW で見る場合は http://www.tains.tohoku.ac.jp/news/ をご指定ください。

お知らせ

2008年4月の組織改編について

2008年4月より，情報シナジー機構は従来よりも広範な役割を持つ組織へと改編され，また情報シナジーセンターはサイバーサイエンスセンターへとその名称を変更しました。それに伴い，TAINSの運用は情報シナジー機構の下で行われることになります。なお，情報部情報基盤課ネットワーク係およびサイバーサイエンスセンターネットワーク研究部は，従来どおりサイバーサイエンスセンター（旧情報シナジーセンター）本館内で業務・研究開発を行い，人員，業務内容，電話番号およびメールアドレスに変更はありません。

本件についての問い合わせ先 tains［AT］tains.tohoku.ac.jp
情報部情報基盤課ネットワーク係
サイバーサイエンスセンターネットワーク研究部

情報シナジー機構の改編について

情報シナジー機構長　鈴木陽一 [1]

情報シナジー機構は全学の情報基盤の一層の充実・高度化の要請に応えるために，平成 20 年 4 月より新しい役割に対応するよう改組され，新体制で臨んでいます。

情報シナジー機構は，平成 13 年 4 月，本学における情報関連組織の総合的協働体として，教育研究活動及び運営を支援することを目的に設置され，国立大学の法人化後も，引き続き本学の情報化の推進に寄与してきました。しかし，情報化社会の進展に伴い，教育・研究と法人運営のための情報基盤の一層の充実・高度化が求められ，その要請に即時的確に対応することが求められるようになってきました。

そのような状況の中，本学総長の「井上プラン 2007」に基づき「情報関係組織の機能点検プロジェクト・チーム」において鋭意検討が重ねられた結果，平成 19 年 11 月に方策がまとまり，情報シナジー機構が担うべき役割の再定義が行われました。その新しい機構の役割は，

1. 本学全体の情報基盤整備等に係る企画立案，調整及び協議，
2. 情報基盤整備実施の担当と，情報システムに係る整備，運用及び管理に関する調整，
3. 情報基盤に基づく各種のサービス提供により，本学の情報化の推進を図ること，

です。つまり，本学に存在する各情報関連組織をよりスムーズに連携させ，より高度な情報インフラを整備し，各情報資産を利用するユーザに対し安全な情報アクセシビリティーを提供することを目的とし，従来の機構の役割よりも，広範かつ積極的な対応が求められ，平成 20 年 4 月から改組して取り組むことになりました。

その取り組みの一つとして，情報シナジー機構に

- ネットワークワーキンググループ
- 認証ワーキンググループ
- ポータルサイトワーキンググループ

の 3 つのワーキンググループが置かれました。ネットワークワーキンググループは，次世代 **TAINS** の導入に向けて，仕様検討や調達作業等を着々と進めています。認証ワーキンググループでは，全学的な統合認証基盤の確立に向けて，集中的な検討や調達作業等が続けられています。ポータルサイトワーキンググループは，平成 20 年 6 月に設置された「業務改革推進タスク・フォース」及び平成 20 年 11 月よりそれを引き継いでいる「業務改革推進室」とも綿密な連携を取りながら，業務システムの総合的な窓口となるポータルサイトの構築に向けて，種々の検討を行っています。いずれのワーキンググループも，様々な部局の有識者が広く集まって，全学的な協力のもと，オール東北大で議論・検討がなされています。なお，これらの情報化推進の実施状況については，平成 20 年 9 月 10 日の部局長連絡会議にて，ご説明しているところです。今後は，情報シナジー機構に置かれた情報シナジー広報室のウェブページ等も活用するとともに，情報システム利用連絡会議等の場でも広報してゆきます。

なお，情報セキュリティポリシーについては,「情報セキュリティポリシー策定委員会」でその策定が検討されてきましたが，関連規程についても改組後の機構と関連づけて検討が続けられています。

[1] 東北大学電気通信研究所教授

情報シナジー機構は，上述の 3 つのワーキンググループにおける検討結果を効率的・効果的に全学の情報基盤として実装してゆきます。また，今後の新たな諸課題に対しても積極的に対応し，本学の情報化のさらなる発展に寄与してゆきたいと考えています。このような仕事を進めるにあたり，情報シナジー機構は,「全学的情報化推進経費」を原資としています．この原資には，今春の「全学的基盤経費」の創設に伴う部局の負担増のうち，およそ半分の金額が投入されていると理解しており，その意味でも大きな責任と期待を感じつつ，任務の遂行にあたっています．今後も全学の皆様のご理解と，ご協力，ご鞭撻(べんたつ)を心からお願いする次第です。

次世代 TAINS の概要紹介

サイバーサイエンスセンター　水木敬明
サイバーサイエンスセンター　曽根秀昭

1　はじめに

前号（TAINS ニュース No.35）の記事 [1] でお知らせしていますように，現在，TAINS/G の次の世代の学内ネットワークシステム，すなわち次世代 TAINS の導入に向けて，集中的に作業が進められているところです。次世代 TAINS は，2009 年 3 月を納入期限としており，来年度早々に本格的な運用を開始できる見込みです。本稿では，この次世代 TAINS について，現時点でお伝えできる範囲で，その概要を紹介します。

以下，本稿の構成は次の通りです。まず 2 節では次世代 TAINS の導入に向けた背景や経緯について現在の状況とともに簡単に記し，次に 3 節で現行の学内ネットワークシステムである TAINS/G の最近の状況について述べます。4 節では次世代 TAINS のネットワーク構成について，5 節では次世代 TAINS への移行方針やスケジュールについて，6 節ではネットワークサービスについて説明します。

2　次世代 TAINS の導入に向けた背景・経緯

本節では，次世代 TAINS の導入に向けた背景や経緯について，昨年度から現時点までの動きと現状を述べます。

2.1　ワーキンググループ等の動き

2007 年 6 月に総長室の下に設置された「情報基盤アクションプラン策定プロジェクト・チーム」は，井上プラン 2007 に基づき,「東北大学情報化推進アクションプラン[1]」を 2007 年 11 月に策定しました。このアクションプランの中では，四つの重点施策の一つとして全学ネットワークシステムの計画的整備が掲げられています。この提言を受け，学内の各部局のネットワークにかかわる有識経験者から構成された「全学ネットワークシステムプロジェクト・チーム」が情報担当理事の下に設置され，2008 年 1 月〜3 月の間に集中的に活動し，次世代の TAINS の導入に向けた基本的な考え方や仕様・整備方針がとりまとめられました。

その後，情報シナジー機構が改組され新たに設置された 2008 年 4 月以降は，機構の中の「ネットワークワーキンググループ」が，全学ネットワークシステムプロジェクト・チームにおける議論・検討・課題等を踏襲しています。このワーキンググループのメンバー構成もまた，学内の各部局においてネットワーク運用で活躍されている有識な経験者が集い，活発な議論や検討が行われています。その過程で，総長室や，学内の関係する部局長から構成される情報シナジー機構・全学情報化戦略会議より貴重なご指導・ご助言を頂戴（ちょうだい）し，あるいは情報システム担当理事や情報シナジー機構長と連携しつつ，ネットワークワーキンググループ，サイバーサイエンスセンターおよび情報部情報基盤課が一体となって次世代 TAINS の仕様策定に必要な事項を検討し，また財務部や施設部を始めとする学内の多くの皆様の全学的な協力のもと，2009 年 3 月の導入を目指して，仕様策定や調達にかかわる作業等が着々と進められてきました。

[1] 総長室のウェブページ（学内限定）で見ることができます。

2.2 予算・経費面の状況

予算・経費の側面について少し説明します。

ご存知のように，1988 年にスタートして以来，三世代にわたる **TAINS**，すなわち **TAINS88**，**SuperTAINS**（1995 年）および **TAINS/G**（2001 年）は，歴代の総長を始めとする諸先生および事務局等のご尽力により，文部科学省（文部省）の深いご理解を得て，補正予算等により整備・拡充されてきました。しかし，2001 年の **TAINS/G** の整備以降は，他の国立大学における状況と同様に，そのような予算獲得が非常に難しい状況になりました。もちろん，現在に至るまで，特別教育研究経費等の予算要求を継続して行っていますが，厳しい状況です。

上述のような状況の中，2007 年 6 月に，同じく井上プラン 2007 に基づき総長室の下に設置された「全学的な基盤経費化プロジェクト・チーム」のご尽力により，基盤的な経費のシステムの構築が検討され，その後，全学的に「全学的基盤経費」の措置が承認されました。全学的基盤経費の内訳は多岐にわたりますが，その内の一つに「全学的情報化推進経費」も含まれました。この全学的情報化推進経費（の一部）を財源とすることにより，**TAINS** の更新が現実化しました。総長室や財務部を始め，ご尽力いただいたご関係の皆様，また各部局の皆様の深いご理解に厚く御礼申し上げます。

なお，全学的情報化推進経費のうち，ネットワークシステム **TAINS** の計画的整備に充てられるのはその “一部” であり，全学的な各種業務の向上や業務効率化のための，全学統合認証システムやポータルサイトの構築その他にも充てられます。繰り返しになりますが,「全学的基盤経費」の一部が「全学的情報化推進経費」であり，その「全学的情報化推進経費」の一部が **TAINS** の更新に充てられます[2]。

また，後ろの 4 節以降でより詳しく説明していきますが，今回の **TAINS** の更新・整備は，予算規模からの制約により，いわゆる「スモールスタート」を基本としていて，ネットワーク機器については，**TAINS/G** と同様に，幹線部分の更新になります。すなわち，例えば各建物の各階におけるネットワーク装置を更新の対象に含めることは予算が足りず，そのような手当は，これまで同様，各部局の分担になります。フロアスイッチや無線 LAN アクセスポイント等のユビキタスアクセス系を含めた真に全学的な整備のための概算要求を今後とも続けていく所存ですので，皆様のお力添えやご協力を何とぞよろしくお願い申し上げます。

3 TAINS/G の最近の状況

次節以降で次世代 **TAINS** の概要を紹介していきますが，それに先立ち，本節では **TAINS/G** の最近の状況を記します。

まず，現在稼働中の **TAINS/G** のネットワーク構成を図 1 に示します。2001 年 12 月の完成の後，各部局からの要望・ご相談により構成の変更や新技術による増強・効率化を重ね，現在の形に至っています。

この図 1 の通り，**TAINS/G** の基幹ネットワークでは，片平，川内，青葉山北，青葉山南，星陵，雨宮の各キャンパスが相互に接続されており，川内〜青葉山北〜青葉山南〜川内と川内〜星陵〜片平〜川内の 2 つのループが川内キャンパスで交わるようなイメージのバタフライ型の幹線ループに，雨宮キャンパスへの延長を持つ構成になっています。各キャンパスの拠点であるノードにはルータ BR が設置され，キャンパス内の副拠点であるサブノードにはスイッチ BS が設置されています。各インハウスネットワーク（部局等のネットワーク）は，各キャンパスのノード（あるいはサブノード）のルータ BR（あるいはスイッチ BS）に 1 Gbps

[2]全学的基盤経費に対する各部局の負担のうち，概算で，実質的にはその約 2/9 が **TAINS** の経費に充てられます。詳細については（学内の皆様は）2007 年 11 月 19 日の「全学的基盤経費（仮称）等に係る会議」および 2007 年 12 月の部局長連絡会議の資料等をご確認下さい。

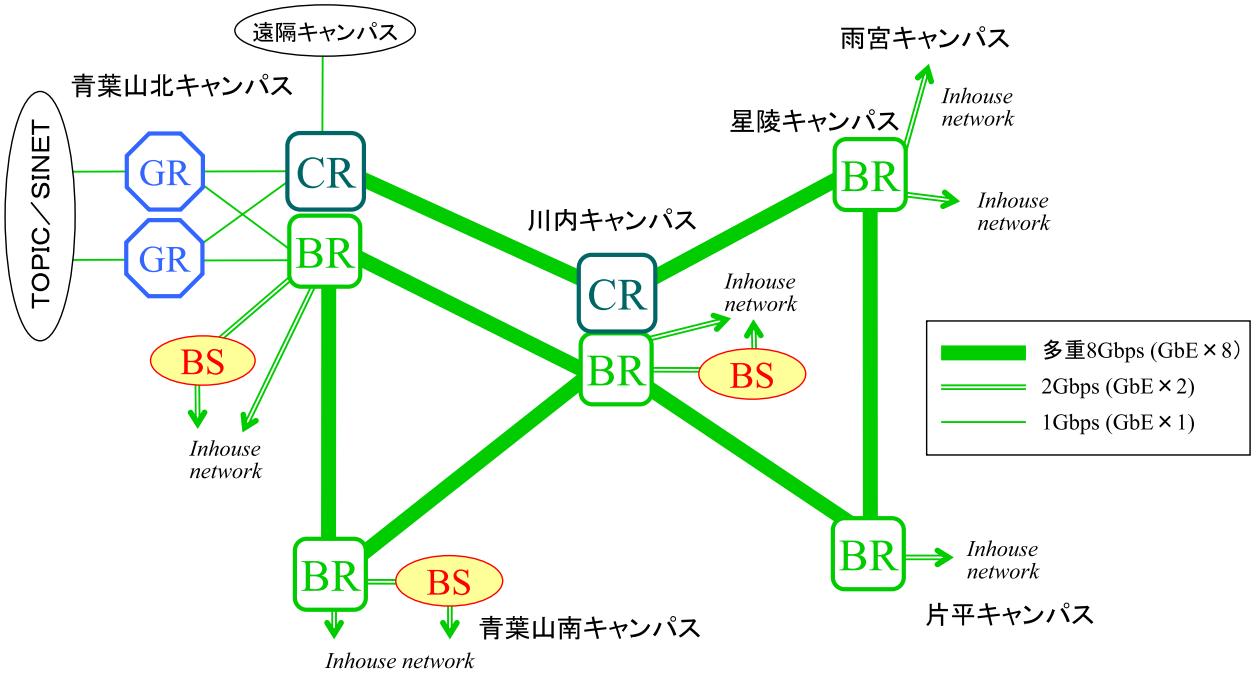


図 1: 現在の TAINS/G の基幹ネットワーク構成概要

の速度[3]で接続しています。また，いわゆるインターネット方面へは，ルータ GR を介して外部ネットワーク TOPIC さらに SINET3 へ接続しています。

この TAINS/G は，2001 年 12 月に導入されたもので，当時の最先端な技術を用いた堅牢（けんろう）なネットワークシステムとして構築されました。そのため，運用開始後から基幹ネットワークを構成する各機器において障害や故障はほとんど無く，極めて順調にネットワーク機能のサービスを提供してきました。しかし，導入からもうじき 7 年になろうとしている現在，さすがに経年劣化は避けがたく，ここ 1〜2 年は老朽化による機器の故障や障害が頻発しつつあり，安定なサービスの継続が危ぶまれています。

TAINS の利用者の皆様で，実感として老朽化した TAINS/G によりサービスが危ぶまれていると感じている方は，いないでしょう。基幹ネットワークの故障・障害が目に見える形で現れていない理由としては，TAINS/G には，巧みな堅牢（けんろう）化が成されていることが挙げられます。例えば，仮にルータ BR の電源モジュールが一つ壊れても，もう一つのモジュールのお陰で “ネットワーク停止” とはならなかったり，一箇所で障害が発生しても，経路の冗長化のためにサービスが継続できたりしています。

そうは言っても，既に TAINS/G のネットワーク機器の老朽化は進んでおり，現在の構成機器では補えないサービス障害が発生する前に，TAINS/G から次世代の TAINS へ切り替える必要があります。

4　次世代 TAINS のネットワーク構成

本節では，2009 年 3 月導入予定の次世代 TAINS について，現地点で仕様等により確定しているネットワーク構成を説明します。今回導入する次世代 TAINS の大きな特徴としては，シンプルなネットワーク構成によ

[3] インハウスネットワークによっては，別な速度で接続しているところもあります。

る堅牢化の継承と，インハウスネットワークを柔軟に収容する多様な発展性，その二つを備えている点が挙げられます。これらの特徴により，安全・安心なネットワークのサービスを安定的に提供し，将来における内外の変化を柔軟に吸収しつつ，効率的・効果的にサービス提供を継続できると考えています。光ファイバの工事や，以下で述べます “エッジルータ” の設置作業のために，各部局の担当者に調整等をお願いすることになりますので，ご理解とご協力をお願いします。

次世代 **TAINS** の基幹ネットワーク構成の概要を図 2 に示します。

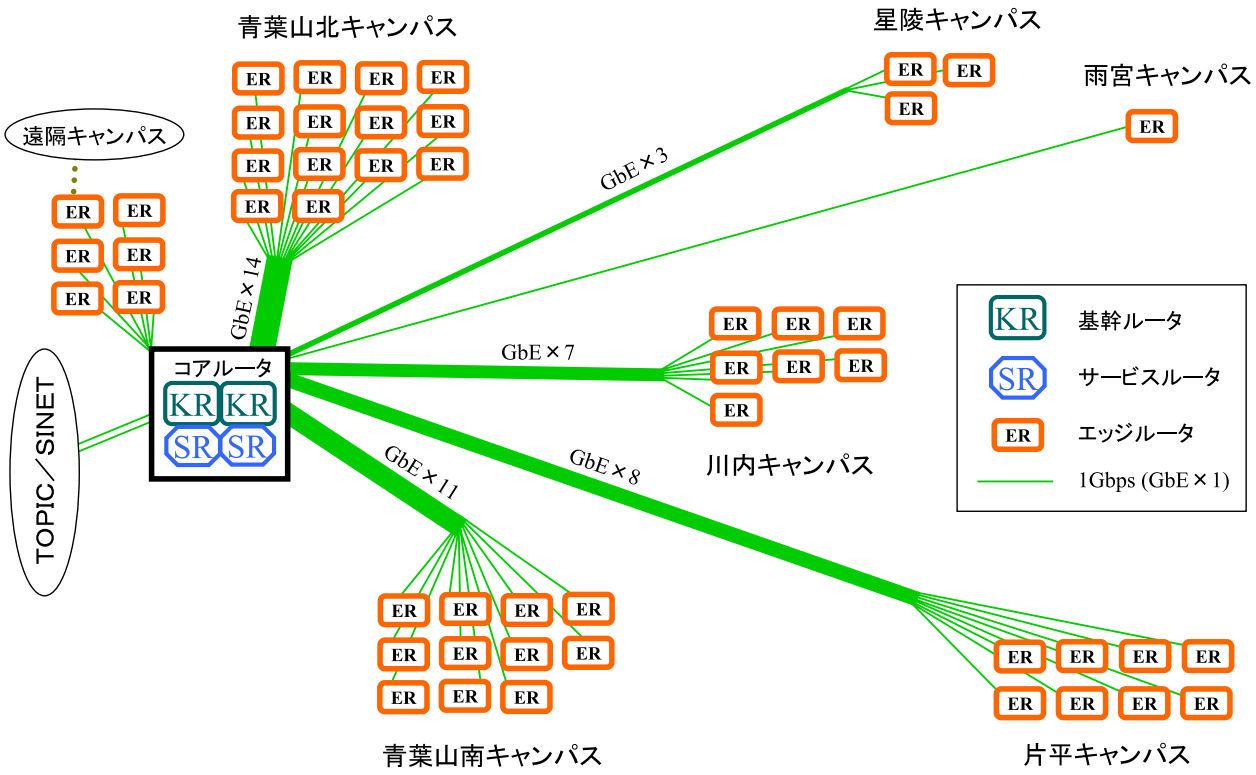


図 2: 次世代 **TAINS** の基幹ネットワーク構成

前節で述べました通り，現行の **TAINS/G** の基幹ネットワークはバラフライ型になっていますが，次世代 **TAINS** では，図 2 の通り，青葉山北キャンパスのサイバーサイエンスセンター内に置かれる「コアルータ」を中心とした，スター状のネットワーク構成となる予定です。コアルータは，基幹ルータ KR とサービスルータ SR から構成されます。基幹ルータ KR は，各キャンパスの主要な（接続点となる）建物[4]に置かれるエッジルータ ER を収容するとともに，外部ネットワーク TOPIC/SINET3 へ接続するゲートウェイになります。サービスルータ SR は，各種の基幹サーバ等を収容するサービスセグメントを構築したり，セキュアなプライベートネットワークを構成して提供するのに用います。各インハウスネットワークは，エッジルータ ER に 1 Gbps の速度で接続することにより，新しい **TAINS** へ移行することになります（詳細については次節で説明します）。

ここまで説明したように，次期 **TAINS** は極めてシンプルなスター状の構成となり，途中の中継ノードを置く他キャンパスにおける機器故障や停電等の影響を受けにくい構成と言えます。一方，経路の冗長化に関し

[4] ここで言う “主要な” 建物とは，ネットワーク的な観点（物理配線経路やトラフィック量等）に基づくものを意味します。

て，今回の構成でもキャンパス間ファイバの物理的障害に対する堅牢性は損なわれず，途中の機器を中継しないことによるシステム障害に対するメリットが得られるものと判断しました。

また，TAINS/G の構成図（図 1）と新 TAINS の構成図（図 2）でお分かりのように，ネットワークの速度はほとんど変わらず，インハウスネットワークの接続収容も 1 Gbps の速度を基本としており，双方で同じです。反面，エッジルータ ER で収容できるネットワークの接続の数は，TAINS/G のインハウスネットワーク接続より拡大されるので，多様な形態でネットワークを使いわけるのに適した構成になります。つまり，今回の次期 TAINS は，スモールスタートから始まり，多様に発展していくことができます。

5　TAINS/G から新 TAINS への移行方針・スケジュール

本節では，TAINS/G から新 TAINS へインハウスネットワークが移行するにあたっての方針や，おおよそのスケジュールについて，時間軸に沿って簡単に説明したいと思います。

5.1　2009 年 3 月時点の予定形態

2009 年 3 月の次世代 TAINS 導入時点において，TAINS/G，新 TAINS およびインハウスネットワークの接続関係は，図 3 に示すような形態になります。

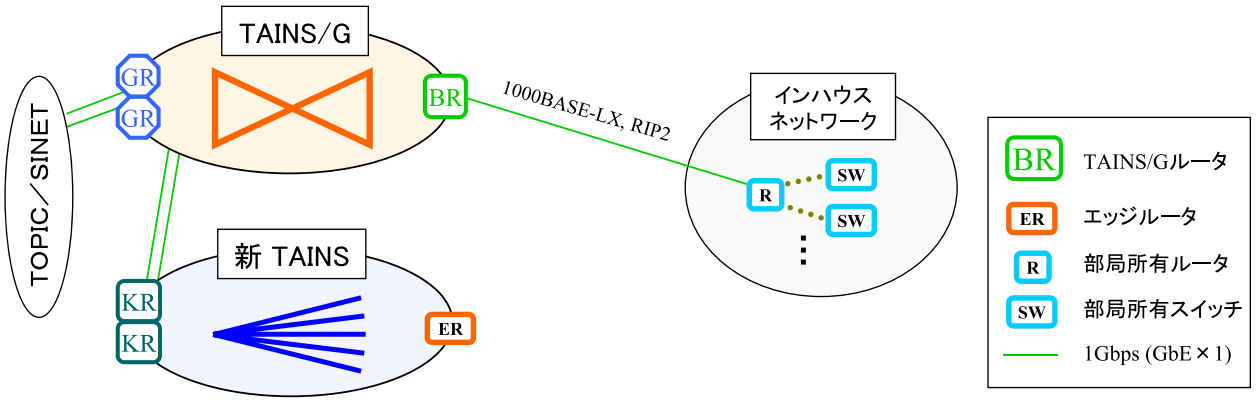


図 3: 新 TAINS の導入時点におけるインハウスネットワークの接続形態

すなわち，導入予定の新 TAINS は，ひとまず TAINS/G に 2 Gbps で接続します。この時点では，インハウスルータ（インハウスネットワークで部局等が所有するルータ）は TAINS/G のルータ BR（あるいはスイッチ BS）に接続したままです。

ちなみに，TAINS/G のルータ BR とインハウスルータは，1000BASE-LX により接続し，RIP2 (RIP Version 2) により経路制御されています [2]。

5.2 2009 年度前半期の予定・計画：インハウスネットワーク接続の切り替え

新 TAINS の稼働開始後から 2009 年度の前半にかけて，各部局のご協力をいただき，各インハウスルータの接続先を，TAINS/G のルータ BR から新 TAINS のエッジルータ ER へ移す作業を進めていきます。

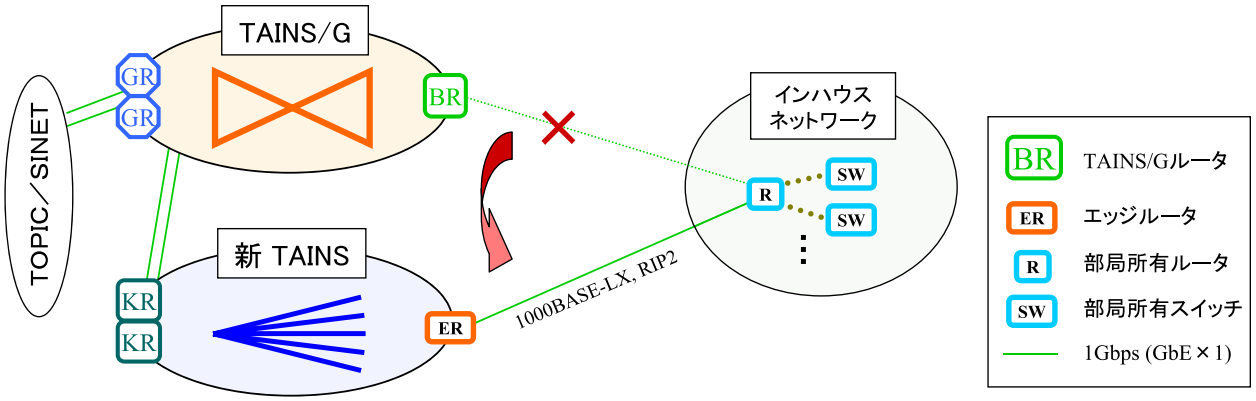


図 4: インハウスネットワークの新 TAINS への接続移行

図 4 に示されていますように，各インハウスルータにとっては，TAINS 基幹ネットワークへの接続先を TAINS/G のルータ BR から新 TAINS のエッジルータ ER へ切り替えることになります。TAINS/G のルータ BR（あるいはスイッチ BS）は各キャンパスのノード（あるいはサブノード）に置かれているのに対して，新 TAINS のエッジルータ ER は学内の主要な建物に置かれます。したがって，今の接続先の BR と，次の接続先の ER の置かれている場所は，多くの場合，物理的に違う場所になることになります。実際には，エッジルータ ER とインハウスルータは，物理的に同じ場所に置かれるケースが多くなります。エッジルータ ER から各インハウスルータまでのライン（光ファイバ等）は，基幹ネットワーク側で調整・確保します。そのために，インハウスルータの位置や接続状況の確認等の現場調査を実施しますので，ご協力をお願いします。

各インハウスネットワークに対する新 TAINS への切り替えのタイミングについては，各インハウスネットワークの担当者との調整により，スケジュールを組んでいきます。今回の移行においては，接続インターフェース (1000BASE-LX) や経路制御プロトコル (RIP2) は変わりませんので，容易に移行できると期待しています[5]。また，切り替えのためにインハウスネットワーク側（部局側）による手当で新たに必要になるネットワーク装置や機器等およびネットワーク配線の工事はありません。

なお，SINET や JGN 等の研究プロジェクト等で VLAN その他により専用線的に TAINS/G を利用している方々に対しましては，個別にご相談することになりますので，よろしくお願い致します。

5.3 2009 年度半ばの予定・計画：外部接続の切り替え

2009 年度前半で全てのインハウスネットワークが新 TAINS に移行した後で，TOPIC/SINET3 への外部接続を切り替えます。すなわち，図 5 のように，TAINS/G のルータ GR による接続から，新 TAINS の基幹ルータ KR による接続へ切り替えます。

[5]前回の SuperTAINS から TAINS/G への移行は，ATM/FDDI から Ethernet への移行でしたので，それに比べれば，今回の移行ははるかに容易であると言えそうです。

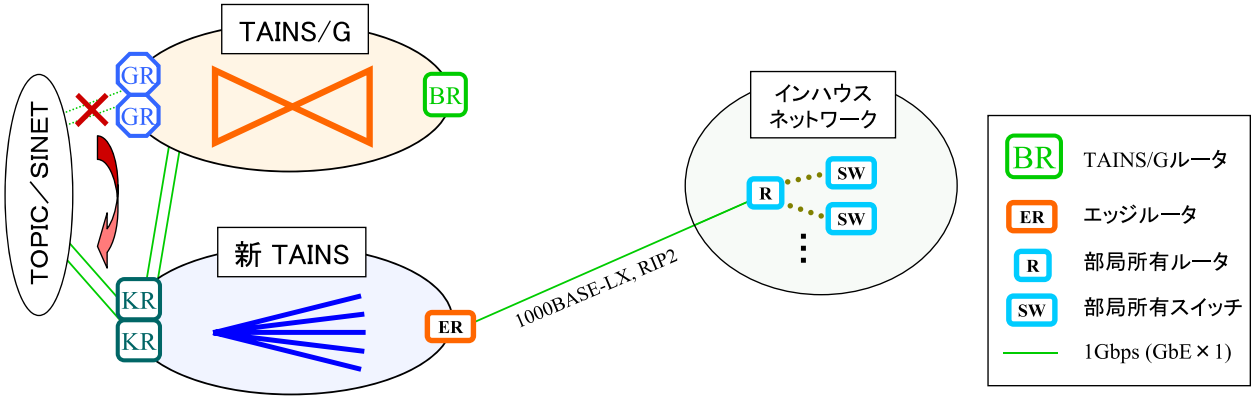


図 5: 外部接続の切り替え

この時点において，TAINS/G の幹線ネットワークとしての役割は終ります。TAINS/G の老朽化が著しいため，図 5 の状態に向かうことを最優先し，5.2 節で説明しましたように，インハウスルータの接続方式を現行のままとして新 TAINS へ切り換えることを当面の目標としています。

5.4　2009 年度後半期以降の予定・計画：インハウスネットワーク接続の高度化

インハウスネットワークの収容に関して，次期 TAINS では，これまでの接続形態（RIP2 による経路制御）に加えて，希望するインハウスネットワークに対しては，ルーティングを基幹ネットワーク側で行うような，L2 接続による収容方式を提供できる予定です。このときインハウスネットワーク側に提供されるサブネットは，ひな形的なアクセス制限を持つセキュアなプライベートネットワーク，あるいは（必要であれば）グローバルネットワークです。

上述のようなインハウスネットワークの L2 収容方式は，インハウスルータの TAINS/G から新 TAINS への移行が全て終わった後で，段階的に提供していきたいと考えています。そのため，いくつかの部局とご相談し，2009 年度前半に先行的にそのような収容形態を試行し，2009 年度後半以降における接続方式のメニューの整理や費用負担の考え方を調整・検討した後に本格運用していく予定です。

なお，新しい収容形態への移行は，希望するインハウスネットワークに対して提供する予定のもので，必要なければ変更しません。

6　ネットワークサービスについて

本節では，ネットワークサービスについて言及します。

まず，DNS サーバや NTP サーバ等の基幹サーバによる既存のサービスは，これまで通りにサービスを継続していきます。その他の既存のサービスには，メールサービスやウイルス対策ソフトの配布があり，これまでは継続的な予算の裏付けがないために継続性が不透明な状況でのサービス提供でしたが，全学的情報化推進経費の制度の期間（当面 2009 年度まで）は安定的なサービスを提供することが可能となりました。

また，メールサービスについては，2009 年 3 月の導入，2009 年度中の本格運用開始を目途に，（事務用 bureau メールシステムの利用者ではない）教職員向けのメールサービスを提供する予定です。これは，情報シナジー機構の認証ワーキンググループで検討されている電子認証基盤の「東北大 ID（仮称）」を活用した

アプリケーションの一つとなる予定で，利用する教職員は “xxx［AT］m.tohoku.ac.jp” というようなメールアドレスを先願主義的に取得でき，メールサービスを利用できるようになる予定です。

さらに，ウイルス対策ソフトの配布を拡充するとともに，スパムメール対策として，部局ドメインのメールサーバ向けにスパマー評価データベースを提供することを検討しています。

加えて，部局ドメインに対して，ウェブサーバやメールエイリアス等のホスティングサービスを提供できる環境の整備を徐々に行います。これについては，2009 年 3 月以降，提供メニューの検討や調整，あるいは費用分担の仕組みの検討のため，いくつかの先行部局において試行することを想定しています。内容が固まり次第，お知らせしていきたいと思います。

7 おわりに

本稿では，次世代 **TAINS** の概要を紹介しました。今回の導入で四代目となるこの新 **TAINS** は，スモールスタートを基本コンセプトとしています。そういう意味では，変化や効果が見えにくいと感じられるかもしれませんが，貴重で限られた全学的情報化推進経費を効果的・効率的に活用していくためにも，次世代 **TAINS** は少しづつ徐々に発展していきます。今後とも，学内の皆様のご理解・ご協力・お力添えをよろしくお願い申し上げます。

謝辞

次世代 **TAINS** の導入にあたり，長時間にわたりご議論やご検討をいただいている情報シナジー機構・ネットワークワーキンググループのメンバーである（筆者 2 名を除く），次の皆様に深く感謝します。

桐原健真氏　（文学研究科）
金谷吉成氏　（法学研究科）
早川美徳氏　（理学研究科）
大町真一郎氏　（工学研究科）
齋藤信氏　（農学研究科）
北形元氏　（電気通信研究所）
木下哲男氏　（サイバーサイエンスセンター）
後藤英昭氏　（同上）
大沼忠弘氏　（情報部情報推進課）
高中寿和氏　（同上）
熊谷功氏　（情報部情報基盤課）
千葉実氏　（同上）
森倫子氏　（同上）
澤田勝己氏　（同上）

参考文献

[1] 水木敬明, 曽根秀昭, “**TAINS/G** の次の世代へ向けて,” **TAINS** ニュース, No.35, pp.3–4, 2008.
(http://www.tains.tohoku.ac.jp/news/news-35/0304.html)

[2] 水木敬明, “**TAINS/G** の完成,” **TAINS** ニュース, No.27, pp.19–21, 2002.
(http://www.tains.tohoku.ac.jp/news/news-27/1921.html)

全学的な統合認証システムの実現に向けて

サイバーサイエンスセンター　木下哲男
大学院理学研究科　早川美徳

1　認証に関係したさまざまな課題

本学の皆さんは，日々の仕事のなかで，以下のような不便や疑問を感じられたことはないでしょうか？(i)「情報システム毎に異なる ID とパスワードを覚えきれないので，何とかこれらを一本化してもらえないだろうか」，(ii)「自宅のパソコンから電子ジャーナルを閲覧できれば助かるのだが … 」，(iii)「最近異動になったはずの職員の連絡先をすぐに調べたいが，どこを見ても掲載されていない」。

このような不便を解消するには，

(a) 本学構成員の電子的な「住民台帳」にあたるディレクトリデータベース，

(b) パスワードや IC カードを用いて確実な本人確認を行うための仕掛け，

(c) 所属や従事している業務に応じて適切なアクセス制限を行うための仕組み，そして，

(d) 使いやすいユーザーインターフェースの提供と，万一パスワードを忘れてしまったような場合でも的確なサポートが得られるような運用体制，

が全学的な情報システムのひとつとして整備されねばなりません。ここでは，こうしたシステムを「統合認証システム」と呼ぶことにします。統合認証システムを情報システムの中枢に据えて整備すれば，研究・教育やさまざまな業務の情報化の推進が期待できますし，先行大学の事例もあります。そして，冒頭で述べた状況からもお判りのように，東北大学においても全学的な統合認証システムが今必要とされています。

2　全学的な統合認証システムの準備状況

本学では,「井上プラン 2007」に基づいて「東北大学情報化推進アクションプラン」（2007 年 11 月）が策定され，その提言に沿って，情報担当理事の下に「全学統合認証システムプロジェクトチーム」（2008 年 1 月–3 月）が設けられました。その活動を引き継ぐ形で 2008 年 4 月から情報シナジー機構の下に設けられたのが「認証ワーキンググループ」で，全学的な統合認証システムの構築に向けて，具体的な検討や，小規模なシステムによる実証実験などを進めてきました。

これまでワーキンググループで話し合われてきた事項は，認証システムの基本的なあり方から，技術的な内容，さらに運用面まで，多岐に渡りますので，詳細は機会を改め，ホームページなどを通じて順次お伝えして参ります。例えば，学生，教職員に今後配布される統合 ID は，ランダムな 10 桁（けた）の英数字列とする予定です。これは，職員番号や学籍番号を元にした ID では，入学年度や所属情報，あるいは，重要な個人情報が，本人が意図することなく漏洩（ろうえい）する可能性があるからです。もちろん，ID と基本的な個人情報はディレクトリデータベース (a) の中で連携され，認証 (b) や認可 (c) の際に内部的に使われます。

本稿執筆段階では，ディレクトリサービスを提供するための基本的なサーバとソフトウェアの調達が進行中であり，来年度早々には全教職員に新しく統合 ID を配布する準備が整う予定です。さらに，次年度以降，

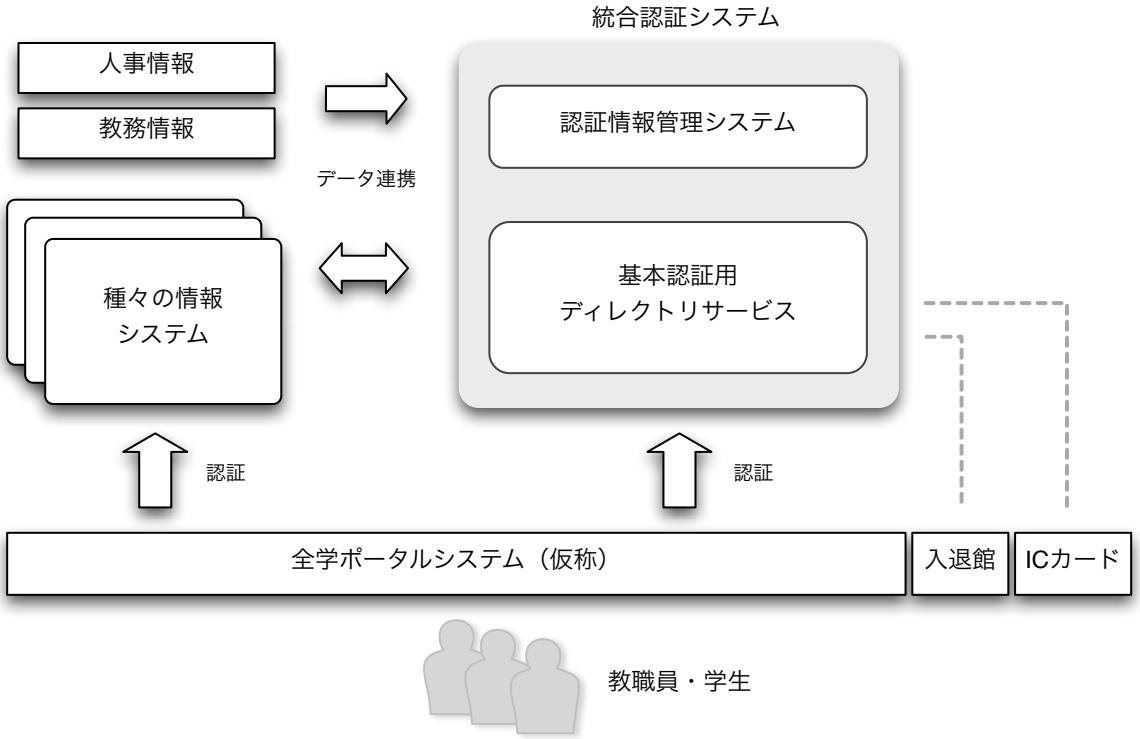


図 1: 統合認証システムのイメージ（計画中または検討中の連携システムを含む）

システムを段階的に増強し，安全性や，レスポンスの向上，さらに堅牢（けんろう）な認証方式にも順次対応していく計画です。

3　これから

統合認証システムは情報システムの基盤であって,「黒子」的な存在ですので，これによって直接的な便益を実感する機会は少ないかもしれません。しかしながら，今後，統合された ID によって，平成 21 年度中に開始される予定の新しい電子メールサービス，各種情報サービスへの「入り口」となる全学ポータルサイト（仮称）へのアクセスが可能となるほか，建物や施設への入退館管理，職員証や学生証の IC カード化とそれを使った各種サービスなども，連携の範囲として検討されています。

最後に強調したいのは，統合認証システムの成否は，情報部門の担当者よりむしろ，人事や教務担当をはじめとする，全ての職員の理解と協力に係っているという点です。統合認証システムは，各種のシステムへの重要な情報提供元となるため，データの完全性や整合性が保証されていることが何よりも大切だからです。

こうした点をご理解いただき，本プロジェクトに対するご支援，ご協力を宜しくお願い申し上げます。

認証ワーキンググループ メンバー

青木孝文（総長室），安西従道（情報部情報推進課），伊藤清顕（情報部），北形元（電気通信研究所），木下哲男（リーダー／サイバーサイエンスセンター），後藤英昭（サイバーサイエンスセンター），酒井正夫（高

等教育開発推進センター），佐藤大（病院），菅原進（総務部人事課），曽根秀昭 （サイバーサイエンスセンター），高橋良（情報部情報推進課），寺澤篤史（情報部情報推進課），中村直毅（大学院医学系研究科），早川美徳（サブリーダー／大学院理学研究科），水木敬明 （サイバーサイエンスセンター），元木正和（評価分析室），森倫子（情報部情報基盤課），横山美佳（附属図書館），吉田幹雄（情報部情報推進課）。

学内ローミングおよび国際ローミングに対応した 情報科学研究科・新無線 LAN システムの構築について

東北大学サイバーサイエンスセンター / 情報科学研究科　後藤英昭

1　はじめに

2003 年の TAINS ニュース No.30 [1]，および 2005 年の TAINS ニュース No.33 [2] において，情報科学研究科における無線 LAN システムの運用について紹介しました。2008 年 3 月の教育用計算機システムの更新に伴い，館内の無線 LAN システムも一新されましたので，その概要を紹介します。

2　複数認証方式とローミングに対応する無線 LAN システム

2.1　ユーザ認証方式の推移

2003 年の初代システムでは，ユーザ認証の仕組みとして Secure Shell 認証方式を採用しました [1]。当時は，無線 LAN システムのユーザ認証機構として企業向けのものが幾つかある程度で，一般ユーザ向けの公衆無線 LAN で利用できるような，手頃（てごろ）で安全なものはありませんでした。このような背景から，筆者らは Secure Shell 認証方式を開発し [3]，当時のシステムに応用しました。この方式は，これまでに他大学等でも利用実績があります。

大学に無線 LAN システムが普及するにつれて，大きな大学では特に，異なる部局にまたがる相互利用の必要性が認識されるようになりました。筆者らは学内における無線 LAN ローミングを実現する方法として，VPN (Virtual Private Network) 技術を応用した「どこでも TAINS」方式を開発し，学内ネットワーク TAINS で利用促進活動を行いました。情報科学研究科の無線 LAN システムもこれに対応すべく，2005 年に機能拡張を行いました [2]。

近年では，ホテルや空港，駅，カフェ，あるいは道路における公衆無線 LAN サービスが普及し，ウェブ認証や IEEE802.1X 認証といった手法が広く使われるようになってきました。教育研究機関向けの国際的な無線 LAN ローミング基盤も立ち上がり，欧州の TERENA で開発された「eduroam（エデュローム）」[4] というシステムに東北大学も 2006 年に接続しました [5]。また，マルチ SSID 対応の無線アクセスポイントの価格低下と普及により，複数認証方式の実現も容易になってきました。

2.2　サポートする認証方式

新システムでは，無線アクセスポイントのマルチ SSID 機能を利用して，次の三種類の認証方式を同時サポートすることにしました。

- 「どこでも TAINS」方式 （VPN 認証方式，学内ローミング用）
- 「eduroam」方式（国際無線 LAN ローミング）
- 「ウェブ認証」方式

情報科学研究科では，他の建物やキャンパスに居住する教員・学生が多いという事情により，ローミングへの対応が欠かせません。大は小を兼ねるという意味では「eduroam」だけでも十分に見えるのですが，利便性を考えると問題があります。「eduroam」では IEEE802.1X による認証（以下 1X 認証と呼ぶ）が標準ですが，1X 認証では端末にインストールするドライバ（サプリカントと呼ばれる）と無線 LAN ドライバ，無線アクセスポイント，認証情報をやりとりする RADIUS サーバの間に不整合や不具合が根強く残っており，まだ安定しているとは言い難い状況です。端末を利用するサイトが変わると，ネットワーク接続の際に認証に失敗したり，しばしばトラブルに見舞われることが経験的に知られています。また，学内でローミングを実現するには，他部局でも RADIUS サーバが整備される必要があります。このため，長年の利用実績があり，安定した環境が提供できる「どこでも **TAINS**」を第一の認証方式として採用しました。

「どこでも **TAINS**」方式では，端末側に PPTP や OpenVPN の VPN クライアントプログラムがあれば良く，特に PPTP 用のクライアントプログラムは MS-Windows XP/Vista，MacOS X，その他幾つかの PDA 等に標準的に組み込まれています。利用者は事前に特殊なプログラムをインストールしておく必要がなく，この点でシステムの利便性は非常に高いと言えます。

一方「どこでも **TAINS**」には，学外のローミングに対応できないという制約があります。訪問者のネットワーク利用の便宜をはかるために，国内でも新しい試みである「eduroam」にいち早く対応することにしました。また，情報科学研究科に無線 LAN のアカウントを作成することで，研究科の教職員や学生が国内外の eduroam 加盟機関でネットワーク利用が可能になるというメリットも生じます。

現在,「eduroam」には欧州で約 30ヶ国，アジア太平洋地域ではオーストラリア，香港，台湾，日本，中国が加盟しており，他の一部の国でも導入準備中です。カナダでも幾つかの大学で利用が始まったようです。

第三の方式の「ウェブ認証」は，他の二方式が利用できない場合の非常手段という位置付けで導入しています。この方式は，また，訪問者向けに一時的に無線 LAN サービスを提供するのに便利でしょう。

「ウェブ認証」は公衆無線 LAN サービスなどでも一般的で，ウェブブラウザを開くだけで ID/パスワードの入力画面が表示されるなど，利用者にとって馴染(なじ)みやすいものです。しかしながら，端末が偽のアクセスポイントを介して偽の認証ページに誘導されるなど，悪意のあるユーザに ID/パスワードを盗まれる危険性が高いというセキュリティ上の問題があります。SSL 対応の認証ページを用いることで，若干のセキュリティ向上策にはなりますが，そもそも多くの利用者がブラウザの http と https の表示の差にあまり気を配らない現状では，偽のページに誘導されても気付きにくいと言えます。VPN 方式や 1X 認証では，端末側の設定を一度正しく行っておけば，基本的にはユーザ認証時に偽のサーバに対して ID/パスワードを通知してしまう可能性はほとんどありません。一方,「ウェブ認証」ではユーザ認証が行われるたびに，利用者の不注意によって ID/パスワードを漏洩(ろうえい)する危険性が生じます。

2.3 システム構成

無線 LAN システムの構成図を図 1 に示します。

無線アクセスポイントは二種類あり，タイプ A が 14 台，タイプ B が 2 台の計 16 台です。従来システムで講義室とリフレッシュスペースに設置されていたアクセスポイントを新製品に置き換えたのに加えて，要望の多かった会議室（一階）と一部の演習室に新規にアクセスポイントを設置しました。アクセスポイントの写真を図 2, 3 に示します。すべてのアクセスポイントが 11b/a/g の無線規格に対応しています。

それぞれのアクセスポイントでは，マルチ SSID の機能を有効にして，前述の三種類の認証方式に対応した SSID を付与しています。具体的には，タイプ A のアクセスポイントにおいて,「どこでも **TAINS**」の SSID が

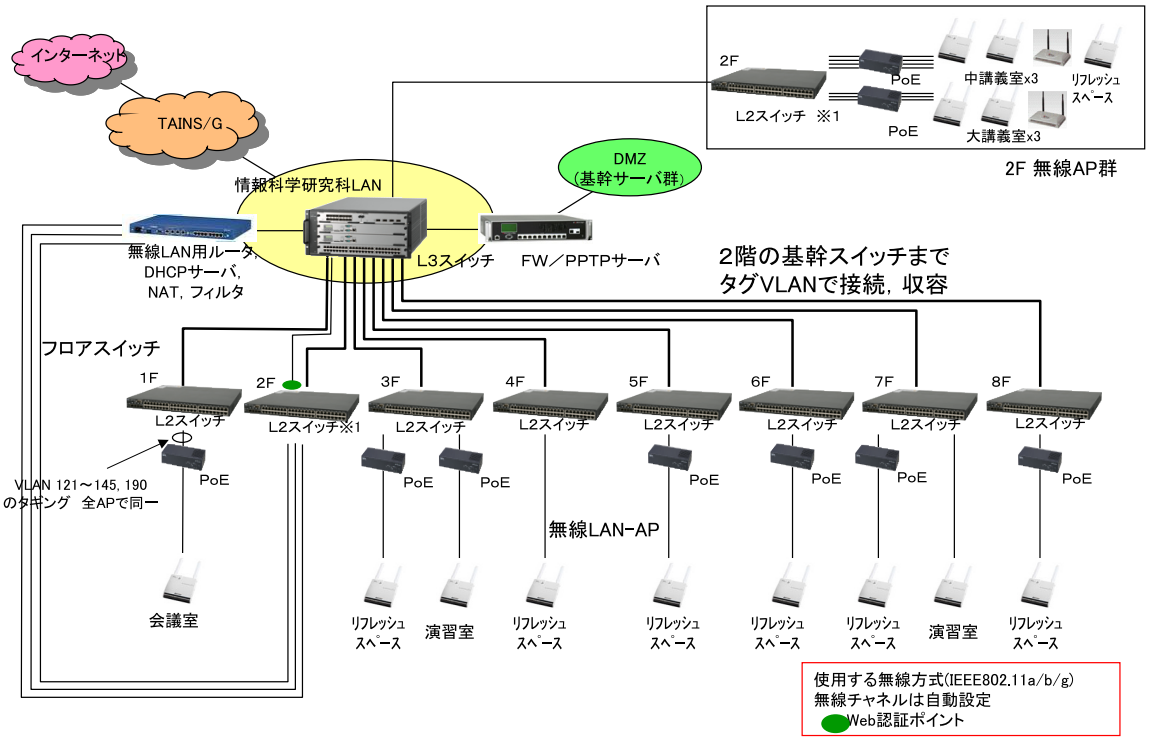


図 1: 情報科学研究科無線 LAN システム構成図（NEC ソフトウェア東北様より提供）

図 2: リフレッシュスペースの無線 AP

図 3: 講義室の無線 AP（タイプ B）

“tains-xF”（x は階番号）,「eduroam」が “eduroam”,「ウェブ認証」が “gsis” に設定されています。

大変残念なことに，調達によって導入されたタイプ A の機種では，製品の仕様により SSID が一つしかブロードキャストできないことが判っています[1]。SSID がブロードキャストされていない（ビーコンが出ていない）場合，利用者が事前に SSID を端末に登録しておかないとアクセスポイントに接続できず，無線 LAN のドライバによっては SSID が登録されていても接続できないという問題が生じることがあります。このため，企業での利用では大きな問題にならなくても，キャンパス無線 LAN や公衆無線 LAN では，SSID がブロードキャストされていないことは利便性の大幅な低下を招きます。また，当該モデルでは，二個目以降の SSID について暗号化を無効にできない，利用できる認証方式に制約があるなどの問題も知られています。

そのため，やむを得ず，以下の方針でタイプ A のアクセスポイントを運用することにしました。

- 学内で利用頻度が高い「どこでも **TAINS**」は，暗号化や WEP を使えないので，プライマリの SSID とする。SSID はブロードキャストする。
- 「eduroam」は標準的な SSID として “eduroam” が広く知られているので，端末側に SSID が設定されていることを期待する。
- 「ウェブ認証」では利便性の観点から暗号化や WEP を使わない運用が望ましいが，利用頻度が低いとみなし，SSID “gsis” と共通の WEP キーを公開する。

しかし，SSID が見えない状態で接続に失敗する端末が無視できないことから，需要が多い講義室については，タイプ B のアクセスポイント（アライドテレシス AT-TQ2403）を別途導入・設置して,「eduroam」と「ウェブ認証」の SSID もブロードキャストできるようにしました。タイプ A との混同を避けるために，SSID はそれぞれ “eduroam2”，“gsis2” に設定されています。

マルチ SSID では，SSID ごとに異なるタグの付いた VLAN がアクセスポイントから出てきます。すなわち，タイプ A では三種類のタグが付いた VLAN が一つの tagged port から出てきます。このタグ付きのネットワークを各フロアにあるスイッチに収容し，タグをばらさないで二階の基幹スイッチまで引いています。

VLAN は二階のスイッチでタグを外され，それぞれの認証方式に対応したゲートウェイや認証スイッチに送られます。無線 LAN 用ルータにおいて,「どこでも **TAINS**」や「eduroam」で必要なフィルタリングを施し，DHCP による端末へのアドレス付与や，アドレス変換 (NAT) を行っています。「どこでも **TAINS**」のフィルタリングに関しては，文献 [6] を参照して下さい。「eduroam」に関しては VPN-only ポリシを採用しており，主要な VPN プロトコルのみを通すようなフィルタが適用されています [5]。

「ウェブ認証」の機能は，市販の認証機能付きのスイッチ（認証スイッチ）を用いて実現しています。少しでもセキュリティを高められるように，認証画面では SSL を使うようになっています。スイッチには，国立情報学研究所と 7 大学の情報基盤センター群による UPKI 構築事業で提供されているサーバ電子証明書 [7] を導入し，標準的なブラウザで警告が出ないようにしています。これにより，予めブラウザに証明書を登録する必要がなくなるとともに，初回のログインにおいて利用者が偽のサーバから偽の証明書を掴(つか)まされる危険性が低くなります。

当システムには,「どこでも **TAINS**」や学外から使えるような VPN (PPTP) サーバも含まれます。VPN サーバ用のアカウントは，基幹サーバ群と連携するような構成になっています。「eduroam」と「ウェブ認証」で利用する RADIUS サーバも，アカウントを共用しています。すなわち，基幹サーバにアカウントを作成すれば，世界中の eduroam 対応サイトでネットワーク接続が可能になります。なお，UNIX 系のアカウントと

[1] 今回，私は調達に関わっておらず，当該モデルの納入を回避することができませんでした。納入業者に非はありません。

RADIUS 用のアカウントの同期が難しいのと，システムとネットワークではログインのセキュリティレベルが大きく異なることに配慮して，無線 LAN/VPN 用のアカウントは UNIX 系と別に作成するようになっています。

3　おわりに

本稿では，学内の無線 LAN ローミング「どこでも TAINS」および国際無線 LAN ローミング基盤「eduroam」に対応した，情報科学研究科棟の新無線 LAN システムを紹介しました。

今回構築したシステムでは，館内ネットワークのスイッチのタグ VLAN 機能を利用することによって，階をまたがる無線 LAN 専用の線を省略し，導入コストが低くなっています。また，このネットワーク構成には，アクセスポイントのマルチ SSID 機能を使っても，物理線をほとんど増やさずに済むという利点もあります。より大規模なシステムでは統合型の無線 LAN 製品を利用すべきでしょうが，小規模なシステムでは本稿で紹介したような構成でも十分だろうと思います。

これから無線 LAN システムを整備する部局においては，ぜひローミング対応のシステムを構築することをお奨めします。

謝辞

当無線 LAN システムの構築にあたっては，以下の方々にご協力をいただきました。紙面を借りてお礼申し上げます。

NEC ソフトウェア東北株式会社 第一ソリューション事業部　佐藤 佳彦 様
NEC ソフトウェア東北株式会社 第一ソリューション事業部　高橋 昭 様
NEC ソフトウェア東北株式会社 第一ソリューション事業部　山本 英樹 様

参考文献

[1] 後藤英昭, “情報科学研究科における無線 LAN システムの運用について,” TAINS ニュース, No.30, pp.16–26, 2003.
(http://www.tains.tohoku.ac.jp/news/news-30/1626.html)

[2] 後藤英昭, “情報科学研究科における無線 LAN システムの運用について (2) — 「どこでも TAINS」への対応,” TAINS ニュース, No.33, pp.10–14, 2005.
(http://www.tains.tohoku.ac.jp/news/news-33/1014.html)

[3] authipgate – Simple Authenticating Gateway for Linux.
http://freshmeat.net/projects/authipgate/

[4] L. Florio and K. Wierenga, “Eduroam, providing mobility for roaming users,” Proc. 11th International Conference EUNIS2005, 2005.

[5] 後藤英昭, “eduroam の構築と参加方法,” グリッド・UPKI 活用のための CSI 講演会 講演予稿集, pp.31-42, 2007.10.12.

[6] 後藤英昭, 水木敬明, 曽根秀昭, “無線・有線 LAN ローミングシステム「どこでも TAINS 2」,” TAINS ニュース, No.35, pp.5-7, 2008.
(http://www.tains.tohoku.ac.jp/news/news-35/0507.html)

[7] 澤田勝己, 曽根秀昭, “東北大学におけるサーバ証明書発行の試行運用についての報告,” 大規模科学計算システム広報 SENAC, Vol.41, No.1, pp.45-51, 2008.
(http://www.cc.tohoku.ac.jp/refer/pdf_data/v41-1p45-51.pdf)

編集後記

■近年，ネットワーク上のサービスが増加するにつれて，個々のシステムでユーザ情報を管理するという仕組みでは，利便性の低下はもとより，セキュリティの観点でも大きな問題があると認知されるようになってきました。OpenID や認証 API のように，個人の所有する ID をまとめる手段も徐々に普及してきています。一見，単一の ID でシングルサインオンができれば理想のようにも見えるのですが，統合しすぎるのも色々と問題を生じます。適度にやるのが良いのです。

本学を含め，国内の大学等で SSO の実証実験が始まっています。特に目に見えるアプリケーションとしては，電子ジャーナルがあります。既に出版業界では IP アドレスによる認証から ID による認証へのシフトが進んでいます。統合電子認証基盤の整備は，これからの学術情報基盤にとって不可欠なものです。一日でも早くサービスが開始・利用できることを願っています。

(HG)

■早いもので東北大学に来てから 3 度目の年の瀬を迎えることになりました。そんな折，次期全学ネットワークの構築という大きな仕事に携わる機会を頂きました。需要予測，仕様検討，設計，広報，運用，将来計画等のさまざまな課題に微力ながら取り組んでいます。構築を進めるにあたって最も重要なことは利用者の皆様のニーズを尊重しご理解とご協力を得ることに他なりません。今後も利用者の皆様にご意見，ご助言を頂きましたことを踏まえて構築に向けて努力してまいりますので，引き続きのご理解とご協力を賜わりますようよろしくお願いいたします。

(K.S)

TAINS ニュース投稿案内

TAINS ニュースでは皆さんから投稿していただいた原稿についても積極的に掲載していこうと考えております。下記の注意事項に沿って，どしどし原稿をお寄せください。

- 術語以外は常用漢字を用い，新かなづかいを用いて「ですます体」でお書きください。表外字についてはふりがなを振らせていただく場合があります。句読点は,「,」と「。」に統一させていただきます。
- 本文については原則として電子的に提出するものとします。

  方法 1: `tainsnews06［AT］tains.tohoku.ac.jp` あてに電子メールで投稿する。

  方法 2: MS-DOS テキスト形式のファイルとして投稿する。この場合には，プリンタ出力も添えてください。この場合の原稿送付先は次の通りです。

  〒 980-8578 仙台市青葉区荒巻字青葉 6–3
  東北大学サイバーサイエンスセンター内
  情報部情報基盤課ネットワーク係
  TEL: 内線（青葉山）6253 / 022-795-6253
  FAX: 内線（青葉山）6098 / 022-795-6098

  手書きで投稿したい場合には，編集グループあてに事前にご相談ください。

- LaTeX 2_ε 形式の原稿を歓迎します。クラスファイルは
  http://www.tains.tohoku.ac.jp/news/tainsnews.cls
  に置いてありますので，お手持ちの Web ブラウザにより取り出してください。
- 図はトレースの必要のない十分な品位のものを提出してください。図についても PostScript や TIFF 形式で電子的に投稿していただくことを歓迎します。

投稿していただいた原稿は，情報シナジー機構情報シナジー広報室 **TAINS** ニュース編集グループで閲読のうえ採否を判断させていただきます。閲読の結果，編集グループが必要と認めた場合には，原稿の訂正や修正をお願いすることがあります。転載や図版の使用については，著作権者の承諾を得ておくようお願いします。また，投稿された原稿は原則として返却されないこと，**TAINS** ニュースが，東北大学の WWW サービスを通して電子的にも公開されることを，予めご了承ください。

TAINS ニュース 第 36 号

発行日　2008 年（平成 20 年）12 月 25 日
編　集　東北大学情報シナジー機構 情報シナジー広報室
　　TAINS ニュース編集グループ
　　曽根 秀昭，水木 敬明，後藤 英昭，
　　千葉 実，森 倫子，澤田 勝己，北澤 秀倫
発　行　東北大学情報シナジー機構
　　〒 980-8578 仙台市青葉区荒巻字青葉 6–3
　　（東北大学サイバーサイエンスセンター内）