2 月 27 日（11:30-14:30）　JANET 訪問レポート

NII 側参加者：
山地一禎（国立情報学研究所　学術ネットワーク研究開発センター）
片岡俊幸（国立情報学研究所　学術ネットワーク研究開発センター）
樋口秀樹（国立情報学研究所　学術基盤推進部）

JANET 側参加者：
Henry Hughes 氏（Strategic Technologies Division; Middleware Group Manager）、
Mark Tysom 氏（Operations Division; Middleware Operations Group Manager）、
ランチの際の途中参加者：
Tim Marshall 氏（Chief Executive）、Jeremy Sharp 氏（Head of Strategic Technologies)

- **JANET における Hughes 氏と Tysom 氏の役割**

Hughes 氏： FAM と Middleware の運用（Operation）におけるトップ
JANET の運用面としては以下の 3 分野がある：UK Federation；Middleware を使った Roamning サービスである Eduroam モデル；認証（Certificate）サービス（現在移行期にある）

Mark 氏：　FAM の開発面での責任者。特にネットワークへのアクセス、Middleware の Authorisation、Federation のアクセスなどを手がけた。FAM の将来的な開発も。

- **現在の JANET のバックボーン（Backbone）：JANET Fibre Network**

3 つのコア（Ring, core）、8 つの集合点（node）からなる（＊小冊子 Introduction to JANET、P.5 参照）

三つのコアエリア：Northern Ring(イングランド北部・スコットランド)
Central Ring (イングランド中部)
South Ring (ロンドンを含む、イギリス南部)

バンド幅は Northern Ring が 10GB、Central と South を合わせて 40GB。Central と South のアクセス量(traffic)が特に多い。中でも、国内・国外（EU へのコネクションなど）とのリンクポイントのあるロンドンは特に多い。従って、Central と South を合わせて 100GB の回路（Circuit）にする計画中。

インフラ整備としては、IP トランジットでアクセスできるようになった。また、Middleware を使うことにより、より広範囲なサービスを提供できるようになった。

EU 内でのリサーチネットワークである EUGion(?)と相互接続(interconnected)している。

- **運営資金について(樋口さんの調査項目)**

資金源、予算の決定について：

JANET の資金は、基本的に JISC を通して政府から支給されている。

政府がそれぞれの地域の学校や高等教育のネットワークに対してそれぞれ予算を設定し、それを JISC に支給している。資金面での交渉を政府と行うのは JISC であり、JANET は直接交渉をしない。JISC から支給される資金は毎年違うので、おそらく、予算の決定は毎年交渉が行われているのではないか（Hughes 氏）。

接続機関からの経費負担について：

接続機関からの経費負担は求めていない(物理的なネットワークの設置に関して？)。ただし、追加でバンド幅が必要な場合、第三者による接続の場合などは、追加料金を請求する。

バンド幅については、各ネットワークごとに政府のイニシアチブ(initiative)によって決められた限度数があり、それ以上を要求する場合は追加分をチャージ。

コネクションのタイプ、Single connection(小規模の機関など)、Two connections（規模のやや大きい機関）、二つ以上の connections（大規模な機関）によってバンド幅の設定は異なる。が、基本的には、地域ネットワークごとにまとまった単位で割り当てている。地域ネットワーク内で柔軟にできるようになっている。

追加バンド幅に関する料金表は極秘扱いであり（＊Tysom 氏に入手可能かリマインドしてください）。料金設定は、単にバンド幅数のみでなく、地域ごと、距離、コストモデル(?)などによって異なり、かなり複雑。

また、登録の際の Certificate サービスとしてではなく、Membership fee としてのチャージはしている。

＜JANET のネットワーク＞

各機関(大学・研究所)などは通信接続業者と契約し、まず地域ネットワーク（NII の地域ごとの Node に相当）につなぐ。JANET のコアネットワークには、地域ネットワークを通してつながる形。JANET は、ネットワークを構築するための資金を提供している。地域ネットワークは JANET が運用しているものと、コンソーシアムが運用しているものがある。図式としては以下：

JANET のコア(core)ネットワークー地域(regional)ネットワークー各機関のサイト

- **接続機関について(樋口さんの調査項目)**

＊接続機関数と内訳については、それぞれのバンド幅も併記されたプリント(極秘扱い)を参照のこと。

教育・研究機関以外の接続について：

民間企業の接続も可能だが、基本的に教育(初等教育から高等教育を含む)や研究に関係した目的でないとダメ。たとえば、教育関係のコンテンツを製作している BBC、気候変動モデルを研究している私企業、がん研究などを行っている慈善団体（Charity organisation）、ヒトゲノム計画などを行っている企業など。参加すると、例えば、全国 26000 の学校が構成しているコンソーシアムのバックボーンに繋ぐことができるが、各学校に繋ぐことはできない。

これら民間団体に関しては、バックボーンへのフルコネクション、バンド幅、国外へのコネクションなどによりチャージしている。

EU 内では、公的資金を受けたプロジェクトを研究などの目的でない私企業に移譲することができない、という決まりがある（Marshall 氏談）

- **NII の今後の予定についてー実行可能性(feasibility)**

JANET でも、NII と同じようなパイロット(pilot)運用→実際の運用というステップを踏んだ。ただし、パイロットのパイロットもあったので、実際の運用にこぎつけるまでに 2・3 年かかった。また、パイロットの際にも、実際の運用に使うものと同じ Federation を使った（米国ではテストは別のものを使ったとのこと）。

同じものを使用はしたが、パイロット運用の際には、それがテストであると、ユーザーにわかるように示した。

- **コンプライアンス（compliance）とオーディット（Audit）に関して**

JANET では、参加している IdP が正しい情報を提供しているかどうか、（Federation に対して？）保障はしない。ただし、各機関は参加の際に JANET の示した規則(rule)を遵守する(compliance)ことに合意しなければならない。規定には、各 IdP が正しい情報を提供しなければならないことが明記されている。事実を語ること('tell the truth')が原則で、Federation は互いの信頼の上に成り立っている。

コンプライアンスに関して、現状では SP は Federation を信用するしかない。信頼性をどのように証明するかが現在の課題で、第三者のオーディットも可能性としてはあるが、費用が高くつくことなどから現実的ではない。

たとえば、政府の Federation である Government Gateway では、6 ヵ月ごとの第三者オーディットを行っている。Government Gateway は、Shibboleth ではないが SAML を使用しており、市民に対するサービス（確定申告・教育・地方自治体など）を行っている。政府の立場は「利用者全員を信用できるわけではない」というものであり、あるユーザーの信用性が危ぶまれたとき、そのユーザーを一方的にシャットダウンすることができる。その意味で、よりコントロールを握れるといえる。

＜Government Gateway と JANET の可能性＞

現在、Government Gateway と JANET をコネクトするという草案（draft）がある。もし、Government Gateway に全市民が参加した場合、JANET に対しても大きな可能性がある。たとえば、JANET の地域ネットワークで小学校などを結ぶ際に、児童の保護者の ID 認証が Government Gateway でできるようになる。

- **アトリビュート(Attribute)に関して**

JANET として４つのコア・アトリビュートを示しているが、義務的(mandatory) なものではなく、あくまでも推奨(recommendation)である。将来的に柔軟に対応できるように、必要最低限しか提言しないようにしている。前述の参加規定（Rule of membership）のみが、参加者に強制的に課せられた義務である。

- **JISC と JANET の役割**

JISC は様々な助言(法的なものを含む)を与えたり、政策(policy)決定をする機関であり、実際のビジネスの運用は行わない（運用は JANET）。JISC は基本的に高等教育が中心であり、学習や教育への ICT の利用促進（ビデオや E-ジャーナルなどのコンテンツへのアクセス促進など）を図っている。JISC の Federation への関わりは、戦略的な側面である（例：コンテンツへのアクセス向上のためにはどのようなインフラモデルが必要か、など）。

従って、JISC のアジェンダは長期的なものが多く、特定のセクターに対する政策を作ったり、というもの。例えば、現在、すべての研究機関を結んで研究データを相互閲覧できるような標準(standard) やプロトコル（protocol）について考えている。

- **Motivation について**

FAM 導入に際して、UK では Eduserve 社(?)による Athens という既存のネットワークがあったという経緯が背景にある。民間企業によるものだったため、Athens 参加には IdP も SP も料金を支払う必要があった。

その点、Federation は特定のソフトウェアもその他のコストも特に必要なく、特に SP に対しては参加が無料なので、大いにアピールした点である。

- **Federation の将来的な Access Management について**

サービスへの付加価値を増やしていきたい。例えば、

・NAC （Network Access Control？)を使ったアドミッションコントロール

・個人情報(identity)ではなくアトリビュート(attribute)による認証

・RADIUS を Federation スタンダードにする

→ 3-4 年で SAML を RADIUS のインフラに適応させることが可能になるだろう。

・サイト間のインテグレーション(integration)を促進し、IdP サイトにログインしたらそのまま外部サイトにもつながるようにする

→ 今のところ最も利用が多いのは E - ジャーナルなどのコンテンツへのアクセスや、生徒の成績管理などを行う School Space へのアクセス

・‘Simple’ Sign On を目指す

→ SSO はほぼ不可能。ID 入力の回数を極力減らすなど、シンプルにすることでよりよいユーザー体験(user experience)につながる

- **Athens と FAM の違い**

Athens も基本は FAM と同じで、学術コンテンツへのアクセスであるが、実際の利用は E-ジャーナルへの接続が主だった。相違点は、FAM では Federation の証明書（credential）を使うことで、ビデオ会議などへのアクセスができること。FAM ならではのサービスに関しては、詳しくは Web サイトを参照

- **エンドユーザー (End-user)からの反応**

カーディフ大学（University of Cardiff）でのパイロット運用のケーススタディ：

・各ユーザーに、学内 ID と別に Federation ID を発行

・カーディフ大学のポータルから Federation のポータルに自動転送の形をとった

→Middleware を使うことにより、ユーザーに対して Federation の存在を前面に出さず(invisible)、そのために余計な混乱などを回避し、よいユーザー体験を提供できた

- **FAM 導入に際して**

・セットアップにかかる時間・コスト・労力を調査した結果、問題点として、一つの機関内でも、部署ごとに違った E メール方式やデータベースなどが存在することが分かった。

→　FAM を戦略的に使うことで、データベースの集中管理(Central management)ができ、時間・コスト・労力の面でプラスになるととを示した

・FAM のインストール自体はそれほど問題にはならなかったが、既存の混在するデータベースを管理することが問題であった（例：各学部ごとに違うデータベースソフトウェアを使用していた、など）

→　Identity Management を統一するところから始めた

例：ある大学では、複数混在していたデータベースのカテゴリーを、スタッフ・学生・卒業生の 3 カテゴリーに統一した。統一に 3･4 年かかったが、それにより集中管理が可能となった。これを実現するためには、政策決定を行える上層部に働きかける必要がある。

Q：統合データベース（unified database）を持った機関の％は？

A：統合していなくても Federation に参加できるので、把握していない。JANET のメンバーは 670 機関、登録されているユーザーID は 2 百万件以上。ただし、各機関でデータベースなど何を行っているか JANET に報告する義務はない。方向性としては、データベースの統一に向かっているが、現在、確実に統合データベースを持っているといえるのは、LSE とカーディフ大学。

・IdP は各機関ごとに一つ、ID は各ユーザーに一つ一回限りで使用されるべき。

→　ID に関しては、この原則を守れていない機関も存在する（ID が再利用されたり）。このようなセキュリティ違反のリスクは存在する。

- **データ保護法（Data Protection Act）に関して**

英国ではデータ保護法はかなり重要視されており、一般の認識も高い。従って、参加への motivation としても、Shibboleth の利用によりユーザーの匿名性を保てる点は評価された。

JANET 参加の規定にも、データ保護法を遵守することが義務付けられている。もし参加機関がデータ保護法に違反したことが判明したら、法廷の手続きを経ることなく、JANET はその機関を一方的に除名することができる。

IdP が ID 情報を第三者（SP）に提供する際は、その SP との契約時に事前に確認され明記された項目に限る。

- **個人情報の取り扱いについての JANET の推奨(recommendation)**

JANET が強く推奨する方法は、ターゲット ID(target ID)のみを利用すること。これにより、プライバシーは守りつつ、必要情報のみを与えることができる。

また、２つのアトリビュートを提供することが鍵。その上で、もし SP がユーザーの名前を要求してきたら、IdP はそれに対して意義を申し立てることができる。FAM では、ID とユーザーをつなげることができるのは IdP のみ。従って、ユーザーの個人情報を保持していない SP が、個人データを第三者に移譲することは不可能。ただし、ユーザー本人が同意の下に個人情報をＳＰに提供することはできる。

Ｑ：SP の My Space などへの個人情報の書き込みについては？

Ａ：前提として、ユーザーの合意が必要。ユーザーが自ら書き込むわけで、IdP が個人情報の漏洩することにはならない。

Ｑ：NII では ArchViewer(?)をインストールしたが、他のソフトの例はあるか？

Ａ：メタデータに何を使っているかまでは JANET で把握していない。

- **Shibboleth のバージョンについて**

現在 Federation のほとんどが Shibboleth 1.3 を使用しているが、2.0 に移行中。新規参加の機関には 2.0 を勧めている。

- **技術面でのサポート体制**

大学に所属し、技術サポートを外注で行うサポートチームがある。6−7 人からなり、マネージャー、2 - 3 人の技術系管理者（technical administrator）と 2 - 3 人の技術系専門家。

JANET 内のチームは、全体で 12 名ほど。Federation へのアプリケーションをチェックする者、サービスマネジャー、渉外係(liaison officer)、開発担当者など。参加 670 機関のユーザーが 2−3 年ですべてログインするようになることを考えると、決して大きなチームではない。想定されているユーザー数は 180 万人。

Ｑ：始動段階ではどのくらいの人数が必要？

Ａ：JANET では、Hughes 氏と Tysom 氏で始めた。適宜、技術者や法律専門家などにヘルプをお願いした。運用が始動してからは、両氏が自ら地方などのキャンペーンに出かけ、FAM に対する認識を高めた。トレーニングのワークショップなどは、第三者に外注するなどして、仕事の集中を回避した。

- **導入時の問題点**

各機関にそれぞれ既存のシステムがあったため、標準的なインストール(standard install)をどうするか、という問題があった。

例：Shibboleth for Windows などのプロジェクトを行った。

多くの機関が何をしているか理解していないで単に「ダウンロード」ボタンを押している状況だったので、技術面でのサポートが必要だった。以上から、

- 明確なコミュニケーション
- サポート
- トレーニング

が必須であるといえる。

- **WAYF からか、ポータルからか？ - ユーザーの使いやすさの視点から**

多くのユーザーが WAYF を使わないという事実がある。ユーザーにとって使いやすい環境であるために、各機関のポータルからそれぞれのリンクにつなげる形を推奨している。

様々な方法が考えられるので普遍的な解決策はないが、例えば、どのブラウザー／機関から入ってきたのかを問う(hinting)ページなどを設定している。

また、機関によってはポータルからの接続が整備されておらず、ユーザーは WAYF から入らざるを得ないので、WAYF ページを使いやすく整備する必要もある。

カーディフ大学の例：

一ユーザーに対し、学内外のネットワークの両方に使えるユーザーネームとパスワードをひとつ与え、大学のポータルから Federation へのアクセスができるようにした。これにより、ユーザーはユーザーネームやパスワードで混乱することなく利用できた。ユーザーにとっては背後にある技術など見えないほうがよい。

- **Federation を広める際の注意点**

Federation 構築プロジェクトに対する各セクターの認識を高めるべき。各組織に対して Federation が必要不可欠であると認識させる必要がある。そのためには、政策決定権をもつ組織の上層部に働きかけ、コスト面やユーザー体験面などでの利点を説得することが必要。

IdP の立場からは、Athens のような年間契約料金が無い（Athens の契約料金は年 15,000 ポンドほどー契約料金は今年から発生）ところが利点。ただし、一年目はアクセスマネジメントの移行などの経費がかかる。また、アクセスできるコンテンツが増えることも利点。

＊コスト削減に関するプレゼンは特にないが、カーディフ大学のケーススタディを参照のこと。

ＳＰの立場からは、参加料が無料なのでコスト面でのメリットが高い。

英国における Federation の参加シェア	
高等教育(HE: Higher Education)	98％
継続教育(FE: Further Educatio)	55％?
小中学校(school)	50％
＊この％はメタデータへの参加であり、ユーザーの％ではない。	

- **参加機関からの負担金について**

より多くの SP に参加してほしいので、SP に対して負担金を求める意向はない。

将来的に、純粋な教育機関でない IdP に対しては負担金を求める可能性有り。例：図書館や NHS(National Health Service)など

サービスを他のセクター(民間など?)に提供することにより、収益面のメリットが考えられるが、現状では政策的に認められていない。

Q：JANET は IdP のホストになる予定は無いのか？

A：プロジェクトが 2 年ほど先行しているスイスの例から、それは考えられない。スイスでは、ユーザーの所属期機関が IdP になっていない場合に ID を提供したが、多大な時間と労力が必要であり、また、ID 発行してしまうことにより、結果として各機関の参加へのプレッシャーを弱めることにもなってしまった。

各組織にとって、Shibboleth IdP は IT に任せればできることで、管理することもそれほど難しくない。難しいのは Identity Management を行うことであり、政策決定部にそれをまず説得することが必要。大きな機関であればあるほど難しい（例：ケンブリッジ大学では、当初各カレッジが独自のシステムを譲らなかった）。

Q：IdP は IT 部門の人間が運用すべき？

A：体質的に大学内の IT 担当者と図書館員は違う。それを連携させる必要がある。

図書館員はリソースの利用や ID Management(書籍分類など)の経験が豊富である一方、ID Management の一本化の技術的な側面は IT 担当者に頼らざるを得ない。秘訣は、大学組織の上層部に働きかけ、トップダウンのモデルで行うこと。具体的には、パンフレットなどは図書館や IT 部門などに送るほか、学長などにも直接送るなど。

また、図書館員と IT 担当者を同じイベントに参加させることも効果的。

Q＆Aセッションなどでお互いの視点を知ることができるし、グループディスカッションを通して問題点などの共有が図れる。

イベントは、100 人くらいの聴衆に対してパワーポイントのプレゼンを行うものと、最大 50 人(35-40 人程度)までの小さなものとを行った。小さなプレゼンの方がディスカッションなどを通して聴衆が積極的に参加することができるので、より効果的。ディスカッションのグループは 6 人くらいで、図書館員と IT 担当者の両方を混ぜるようにする。

参加働きかけの手紙は、対象者（学校、大学、図書館員、IT 担当者、管理職など）に合わせて違うものを用意した。　＊手紙は公開していないので入手不可

- **JANET の将来的な課題**

・Federation のウェブサイトの開発

・Middleware について

　－技術的な側面ではなく、政策や非教育系機関の参加可能性についての構造など

・メタデータの管理

　－拡大しすぎているので、インターフェースを IdP や SP に送り独自にやってもらうようにしたい

・技術面では、

- inter-Federation

- Eduroam
- Middleware 関連：３Ｇデバイスをつなげるためには、どの framework、どのサイズ（ブロードバンド、WiFi）が最適か、など
- ネットワークのアクセス容量(traffic)に合わせたサービスの模索

- **E-Certificate と保証レベル (Level of Assurance)について**

E-Science Community が E-Certificate に関しては積極的であるが、保証レベル (Level of Assurance)の問題がある。また、もし JANET が E-Certificate を導入しようとすれば、システムを変えなければいけない。JANET としては、高い保障レベル (High Level of Assurance) を実現するためには、SAML にすべきだと考えている。JANET では保証レベル に関するプロジェクトを始めたが、保障レベルに関しては英国政府や米国政府の共通水準が確立されるのを待ち、それに合わせていく必要がある。

前述の Federation のオーディット（Audit）も、保障レベルと関連して行うべき。オーディットをどこが行うかなど、その適格性を考えるのが次のステップであるが、各機関の自己評価（self-assessment）に任せるのではなく、JANET も関わる必要があるだろう。

- **OpenSEA Alliance に関して**

JANET も参加している。また、民間のサプリカント(supplicant)も参加している。（ちなみに、JANET はサプリカントベースの方向に向かっている。）

OpenSEA Alliance により、クロス・プラットフォーム（Cross Platform）の問題も解決できるだろう。また、Federation コンピューティングのスタンダードも構築することができるだろう。

＊　OpenSEA Alliance：http://www.openseaalliance.org/

以上

＊＊

注１：ミーティングの時間軸に合わせてまとめてあります。

注２：名称などで不確実な点は記述の後に(?)を、言い回しや内容で不明な箇所は赤字で記してあります。