

認証フェデレーションに対応したテレビ会議 MCU 予約システム FaMCUs の開発

中村素典^{†1} 西村健^{†1} 山地一禎^{†1} 岡部寿男^{†2}

H.323 国際標準に準拠したテレビ会議端末の普及が進んでいるが、多くの拠点が参加するテレビ会議を行うためには、テレビ会議端末の他に多地点接続装置(MCU)が必要となる。このような装置の価格と利用頻度を考えると、各大学が個別に維持することは現実的ではなく、1 台の MCU を複数の大学で共用することが望ましい。そこで、このような設備の共用を促進するために必要となる共通の予約システム FaMCUs を開発した。FaMCUs は学術認証フェデレーション「学認」の SP として実現されており、学認に参加する大学の教職員であれば自由に予約を行うことができる。また、多様なネットワーク環境からテレビ会議に参加できるようにするため、併せて Skype とのゲートウェイ機能も用意している。本稿では、FaMCUs の設計と実装について述べる。

Development of FaMCUs – A Video Conferencing MCU Reservation System with Federated Authentication

MOTONORI NAKAMURA^{†1} TAKESHI NISHIMURA^{†1}
KAZUTSUNA YAMAJI^{†1} YASUO OKABE^{†2}

Video conferencing systems based on H.323 international standard have been widely deployed these days. When many sites are required to join to a conference with a video conferencing system, MCU (Multipoint Control Unit) is also required to connect them. But such a MCU is expensive and not used so frequently, it is better to share a MCU among universities, rather than having a MCU by each university. So we developed a video conferencing MCU reservation system called FaMCUs to share MCUs among universities. FaMCUs is constructed as an SP of the academic identity and access management federation, GakuNin, and freely reserved a conference room on a MCU by faculty member or staff of a university participating in the GakuNin. We also provides some gateway features such as Skype Gateway to support joining to a conference room from a variety of network environments. In this report, design and implementation of the FaMCUs is described.

1. はじめに

ネットワーク技術や映像音声処理技術等の進歩に伴い、高品位かつ汎用のテレビ会議用システムが安価に提供されるようになってきた。テレビ会議システムを利用することで、会議に参加するために移動する時間と費用を削減することができることから、その需要は次第に増加してきている。

現在、国際的な標準規格である H.323[1]とそのシリーズに準拠したテレビ会議システムの利用が主流であるが、これらは端末間を一对一で接続するための技術であり、3 地点以上を結んだテレビ会議を実施するには、多地点接続装置（以下、MCU）が必要となる。

テレビ会議用端末の中でも高機能なものについては、MCU 機能を内蔵しているが、そのようなものは一般に高々 4~6 地点（当該端末を含む）までしか接続できず、その制御機能も限定的である。より多くの地点を接続した会議の開催や、接続拠点毎の合成画面制御やミュート操作をきめ細やかに行うためには、端末機能が附属しない専用の MCU の導入が必要となる。

このような MCU には、6 地点が収容できる小規模なものから 80 地点が収容可能な大規模なものまで様々あるが、端末装置に比較して一般に非常に高価であり、加えて、テレビ会議システムに関する技術が未だ発展途上にあり機能向上がめまぐるしいことや、MCU の利用頻度を考慮すると、全ての大学や研究機関が個々に保有することは非効率であり、少数のシステムを共用することが望ましい。

このような背景から、本稿では、テレビ会議システムを学術認証連携フェデレーション「学認」を用いて共用するためのシステム FaMCUs (Federation Authenticated MCU Service)[a]の設計について報告する。

2. FaMCUs の設計

2.1 学術認証フェデレーション「学認」との連携

MCU は、複数の機関で共有できるようにすることが効果的であるが、複数機関による共有のためには、アクセスのためのアカウント管理にコストをかけるべきではないが、このような場合には、認証フェデレーションの仕組みの利用が適している。

認証フェデレーションとは、シングルサインオン(SSO)技術を利用した認証連携の仕組みである。ログインのための ID とパスワードの検証を IdP (Identity Provider) と呼ばれ

^{†1} 国立情報学研究所
National Institute of Informatics
^{†2} 京都大学
Kyoto University

a) <https://mcus.nii.ac.jp/>

る 1 台の認証サーバに集約し、サービスを提供する SP (Service Provider) と呼ばれる各サーバは、利用者に対するログイン時の認証処理を IdP に依頼する。IdP を異なる複数の SP で共用することにより、一度認証が済んだユーザに対しては、別の SP にアクセスする際に ID とパスワードの再入力を省略させる、いわゆるシングルサインオンが実現される。この枠組みを、1 つの組織の中で利用するだけでなく、組織ごとに管理される IdP を用いて、組織外から提供されるサービス(SP)における認証においても利用できるようにするサーバ間連携(組織間連携)の枠組みが認証フェデレーションである。SP がこのような枠組みを利用することにより、SP におけるユーザ管理コストが大幅に削減される。学術では、このような枠組みに基づく学術認証フェデレーションの構築が国を単位として始まっており、SAML (Security Assertion Markup Language)[2] が用いられている。日本国内では国立情報学研究所を中心に 2009 年より「学認」の構築が始まっている[3][4]。FaMCUs は、このような学認の枠組みを利用して、複数の組織に対して提供するサービスを容易に構築できることを示すことも目的の 1 つとしており、リバースプロキシとしての試作[5]を経て設計を行った。FaMCUs では、複数の MCU に対する予約の管理が可能であり、現在は 5 台の MCU が予約可能となっている(表 1)。うち 1 台は京都大学に設置されているものであり、国立情報学研究所が予約管理の委託を受けている形となっている。

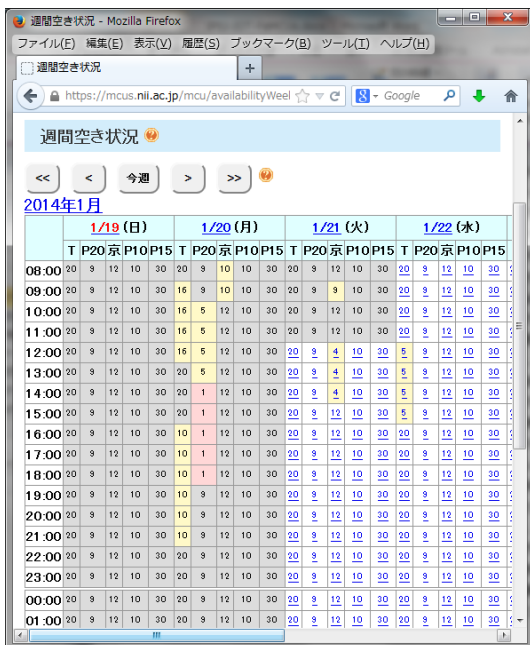


図 1 FaMCUs における MCU 空き状況表示例
 Figure 1 An example of MCU Occupation Status

それぞれの MCU は同時に複数の会議室を予約することが可能であり、同時に予約が可能な会議室の数は、MCU ごとに定められる同時接続可能端末数にのみ制限される。

利用者は予約の際に接続予定の端末数を指定し、予約したい時間帯において接続可能端末数に空きがあれば会議室を予約することができる。利用者は、MCU ごとの空き状況を見ながら、利用する MCU を選択する(図 1)。予約が可能な会議室の開催時間は最大で 24 時間としている。24 時間を超える予約は、複数の予約に分割する必要がある、端末の再接続が必要となる。

表 1 FaMCUs でサポートする MCU

Table 1 MCUs supported by FaMCUs

機種	備考
Polycom RMX 2000	20 ポート (※)
Polycom RMX 1000	20 ポート (※)
Polycom RMX 1500	60 ポート (※), NII 内部利用
Codian 4510	20 接続
Codian 4205	12 接続, 京都大学提供

※1 接続において消費するポート数は解像度に依存する

2.2 属性情報を活用した認可

認証フェデレーションの基盤技術となるシングルサインオンの枠組みでは、IdP において ID とパスワードの確認を行うことで利用者を特定し、SP ではその利用者に対するサービスの提供可否を判断するという役割分担となる。前者の IdP による処理は認証と呼ばれ、後者の SP による処理は認可と呼ばれる。これがいわゆる、認証と認可の分離である。認証フェデレーションでは、SP における認可のための情報として、IdP から SP に対し認証を経たユーザに関する情報を送信する仕組みが提供されているが、このような情報を属性情報(Attribute)と呼ぶ。学認では、17 種類の属性情報を定めている[6]。

FaMCUs では 17 種類の属性情報のうち、IdP からの 2 種類の属性情報の送信を求めている。1 つは eduPerson TargetedID で利用者の識別のために利用される、いわゆる仮名識別子(PPID: Pairwise Pseudonymous Identifier)である。もう 1 つは eduPersonAffiliation で利用者の大学等における身分を示す属性である。この属性は値として学生であることを示す student, 教員であることを示す faculty, 職員であることを示す staff を持つが、FaMCUs では教職員からの予約のみを受け付けるため、認可の際に属性値に faculty あるいは staff を持つ利用者であることを確認している。従って、各組織の IdP 管理者は、FaMCUs という SP に対して前述の 2 つの属性情報を送出するよう設定する必要がある。

なお、利用者は最初のアクセス時に自分のメールアドレスを登録するようになっており、予約完了情報はメールでも通知される。

2.3 代理アクセス機能

上述のとおり、FaMCUs は認証フェデレーションと連携したテレビ会議の会議室の予約を提供しているが、テレビ会議の開催中には、画面レイアウトの変更やテレビ会議端

末の呼び出し・切断等の制御が可能である(図2)。この制御についても、予約を行った利用者が FaMCUs にログインすることで操作可能であるが、一般的に遠隔講義等の場合は、予約した教員には画面レイアウト変更等の操作を行う余裕がなく、講義を補助する TA 等に制御をまかせたい場合が多い。そこで、FaMCUs では予約した会議室に関する操作権限を委譲する仕組みを用意している。

会議室を予約すると、予約情報として、代理アクセス URL が予約者に通知される。予約者は、操作権限を委譲したい人に代理アクセス URL を通知し、委譲を受けた人がその URL にアクセスして FaMCUs にログインすると、その会議室に関する権限が付与され、自分で予約した会議室と同様にアクセスすることが可能となる。FaMCUs は、学生には予約権限を与えていないが、代理アクセス URL を通じてログインした場合は、当該会議室に関する予約に対してのみ権限が与えられる。現在、権限の内容には特に制約を設けていないため、会議室の予約時間の変更や予約の削除も含めて可能となっている。

	Room A	Room B	Room C	Room D
Lecturing from A	A B C D	A	A	A
Q&A with B	B	A	A B	A B
Q&A with C	C	A C	A	A C
Q&A with D	D	A D	A D	A

図3 各拠点における画面合成レイアウト

Figure 3 Screen Composition Layout at Each Location

従来の MCU は、画面合成機能を1つしか持たず、各拠点は同一の合成映像しか受信することができなかったが、近年の MCU の高機能化により、拠点ごとに独立した合成映像を生成することが可能となっている。そこで、FaMCUs では、図3に示すように拠点ごとに最適な画面レイアウトになるようなレイアウト一斉切替機能を実装している。この機能を利用するためには、まず講師がいる拠点を選択する。これにより、講師拠点からの講義モードとなる(図4)。次に質疑応答の状況となった場合は、質疑を行う拠点を質問者のボタンで選択する(図5)。これにより、質疑応答を行う2拠点は互いに相手の映像が大きく表示されるとともに、質疑に参加しない拠点では、質疑応答を行う2拠点の映像が並ぶ映像となる。解除することで、元の講義モードに戻る。



図2 会議室の制御画面

Figure 2 Control Screen of a Conference Room

2.4 画面レイアウト一斉制御

遠隔会議システムは、双方向かつリアルタイムに映像と音声を送信するシステムであることから、遠隔講義にも活用されることが多い。2拠点を結ぶ遠隔講義では、互いに相手の映像を受信して表示するだけであり、送信映像のソースとなる講義室内のカメラ制御のみが重要となる。一方、3拠点以上を結ぶ遠隔講義では、自拠点以外の複数の拠点のうちどの拠点の映像を受信表示するかを選択することや、場合によっては合成表示により1つの画面に同時に表示させるといった制御も必要となる。音声等による自動選択も不可能ではないが、様々な状況を踏まえた安定で的確な制御のためには、人間による手動制御が望ましい。講師自身で制御するのは容易ではないため、TA等の画面制御を行う補助者がいることが望ましいが、システム上で制御ができれば全ての拠点に補助者が1人ずつ居る必要はなく、どこかの拠点に補助者が1人居てシステムを制御できれば十分である。



図4 講師拠点の選択

Figure 4 Selection of Lecturer Location



図5 質疑拠点の選択

Figure 5 Selection of Questioner Location

なお、この機能は、DVTS 用 MCU である quatre を用いた遠隔講義の経験[7]を踏まえたものである。

2.5 モバイル環境支援

様々な場所からテレビ会議に参加できるようにするためには、あらゆる形態のネットワークに対応可能なテレビ会議接続用アプリケーションを提供する必要がある。日頃からノート型 PC を持ち歩いている利用者であれば、PC 用のテレビ会議ソフトウェアを利用することでテレビ会議に参加できるが、主要なソフトウェアは、ネットワーク帯域が比較的確保できていることが条件であったり、制約が厳しいファイアウォールの下では動作しなかったりするという問題がある。最近では、スマートフォンが急速に普及していることもあり、スマートフォン用のアプリを用いた接続への需要も高くなってきている。

Windows PC であれば、当初より FaMCUs で利用している MCU のうち、Codian において ConferenceMe と呼ばれるアプリケーションが提供されている。ConferenceMe では 5082/UDP を通信に利用するが、ファイアウォールで塞がっている場合は TCP 通信にフォールバックする。ただ、特定のウィルス対策ソフトとの相性が良くないという問題が報告されている。

加えて、FaMCUs では、以下に示す 2 通りのモバイル環境の支援を行っている。

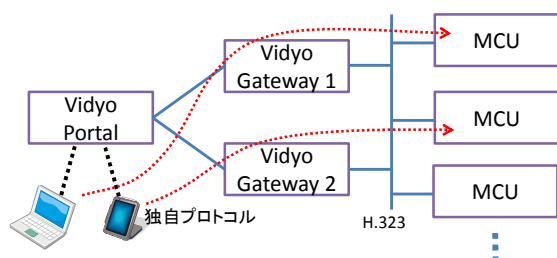


図 6 Vidyo システムとの連携

Figure 6 System Architecture with Vidyo System

2.5.1 Vidyo ゲートウェイサービス

Vidyo 社[b]が提供する PC 用のアプリケーションである Vidyo Desktop やスマートフォン用アプリケーションである Vidyo Mobile はネットワークの帯域が細い場合でも比較的安定して映像・音声の伝送が可能であるとの評価結果を得たことから、FaMCUs において暫定的な実装にてサポートを行っている (図 6)。Vidyo は独自のルーティング技術を利用しているため、直接 H.323 準拠のテレビ会議システムには接続できないが、Vidyo Gateway を経由することにより接続することが可能である。Vidyo Desktop および Vidyo Mobile を利用するためには Vidyo サーバ上にアカウントが必要となるが、Vidyo サーバは認証フェデレーションに対応していないため、Vidyo を利用したい利用者は、事前にアプリケーションをインストールした上で、FaMCUs にお

いて利用時間帯の予約を行う。予約した時間になると、Vidyo サーバにアカウントが作成され有効になるので、アプリケーションからログインした上で、Vidyo Gateway 経由でのテレビ会議接続を指定する。なお、スマートフォン用アプリケーションの現在のバージョンでは、DTMF (Dial Tone Multi-Frequency)の送りがサポートされていないため、最初の接続先の指定時に、会議室番号も含めて指定する必要がある。

2.5.2 Skype ゲートウェイサービス

無料の音声通話サービスとして広く普及しているものに Skype[c]がある。PC やスマートフォンを始めとして幅広いプラットフォームをサポートするとともに、ネットワークの帯域が十分でなくても比較的良好的な音質で通信することができ、比較的制限の強いファイアウォールの下でも利用できることが多い。1 つのアカウントを複数のプラットフォームで共有することも可能である。そこで Skype からテレビ会議に接続する方法について検討を行った。

Skype は独自の通信プロトコルを利用しており、その詳細は公開されていない。しかし、Yester 社から提供されている Skype と SIP[8]サーバを連携させるゲートウェイ製品 SiSkyEE (SiSky Enterprise Edition) [d]を利用することで、Skype からテレビ会議に接続が可能となることが確認できたため、Skype ゲートウェイシステムの構築を行った (図 7)。

Skype の利用者は、ゲートウェイ上で動作する機械応答 skype ユーザを音声通信にて呼び出し、接続後に DTMF を用いて接続先の MCU を選択した後、続けて会議室番号を DTMF で送信すれば、テレビ会議に参加することが可能である。接続先の MCU は、FaMCUs で予約可能な MCU から選択する。現時点で 10 までの同時接続に対応している。

3. 実装

3.1 FaMCUs

一般に MCU はアプライアンス製品であり、独自に SAML に対応させることは容易ではない。そこで FaMCUs では、利用者を認証フェデレーションと連携して認証するとともに、MCU に対する必要な操作を全て中継する機能を持たせる必要がある。FaMCUs を含む全体のアーキテクチャを図 7 に示すが、FaMCUs 自身は、CentOS 5.4 上に Apache 2.2, Shibboleth SP 2.5, tomcat 5, mysql 5 をインストールし構築を行った。Shibboleth[e]は SAML を用いた認証フェデレーションを構築する際に広く利用されているオープンソースである。

FaMCUs では、予約情報の管理を行うと共に、MCU に対して予約情報の転送を行う。また、FaMCUs を介した MCU の操作により、会議中の制御も会議室を予約したユーザの

c) <http://www.skype.com/ja/>

d) <http://www.yeaster.com/products/siskye.asp>

e) <http://shibboleth.net/>

b) <http://japan.vidyo.com/>

権限において可能になっている。FaMCUs から MCU に対する制御は、SOAP により行うが、API の仕様は、Tandberg 社（現在は Cisco 社）および Polycom 社からそれぞれ公開されている[9][10]。なお、Polycom RMX 1000 については、標準では SOAP API が装備されておらず、スケジューリングソフトライセンスを追加購入することで対応する。

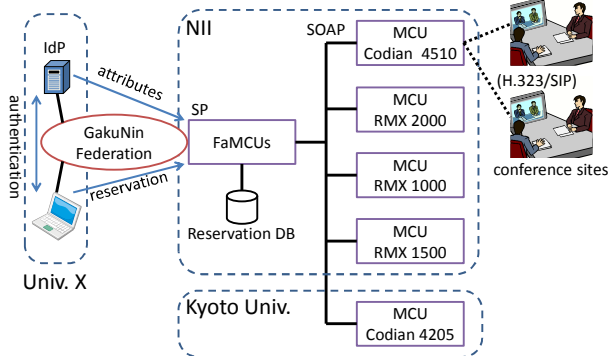


図 7 FaMCUs アーキテクチャ
 Figure 7 Architecture of FaMCUs

3.2 Skype ゲートウェイサービス

システム構成を図 8 に示す。システム構築には、SiSkyEE 2.6.0.1, Skype 3.6.0.244, Asterisk 11.0.1 等のソフトウェアを利用した。Asterisk[f]は VoIP PBX を構築するためのオープンソースである。なお、現在のシステムには以下の制約がある。

- SiSkyEE は Windows XP, 2003 Server までの OS しかサポートしていない
- SiSkyEE は Skype の最新版に対応していない
- SiSkyEE は Skype の映像通信の中継機能を有しない
 また、システム構築時において以下の問題があった。
- SiSkyEE はライセンス登録ができていないと、通話中に“yester”という音声メッセージが定期的に挿入され、会話が阻害される。VM 上の Windows にインストールした SiSkyEE は、再起動等のタイミングでライセンス登録が無効になることがあり、その場合は Yester 社にライセンスの再認証を依頼しなければならない。
- FaMCUs から予約可能な MCU は SIP にも対応しているため、当初、Asterisk と MCU の間の通信に SIP を用いたが、間に存在するファイアウォールの IPS (Intrusion Prevention System)機能により、接続後 5~10 分程度で遮断されるという問題が発生した。IPS において SIP の監視機能のみ OFF にすることができなかったため、試行錯誤を行った結果、Asterisk と MCU との通信を H.323 に変更することで解決できた (Asterisk に ooh323 オプションを追加し H.323 に対応させた)。当該ファイアウォールは、H.323 通信に対しては遮断しないようであった。

f) <http://www.asterisk.org/>

MCU への接続後に DTMF による会議室選択を可能にするためには、SiSkyEE の各ポートの設定において DTMF Mode を RFC2833, INFO method でなく、In-band を選択しておく必要がある。

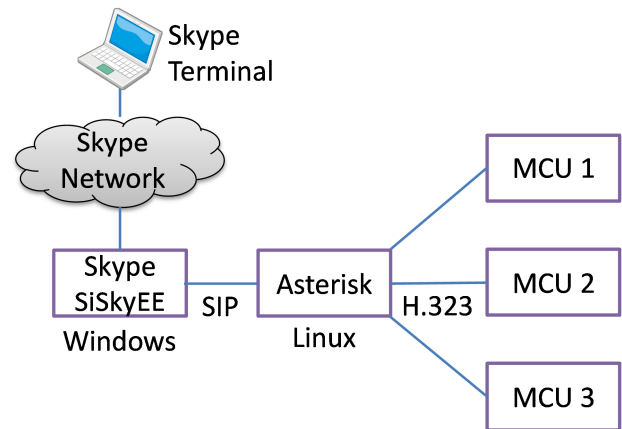


図 8 Skype ゲートウェイシステム
 Figure 8 Skype Gateway System Architecture

4. おわりに

FaMCUs はリバースプロキシによる試作を経て 2009 年度に構築し、2010 年度よりサービスを開始して、日本大学や京都大学での遠隔講義を含め多くの方々にご利用頂いている。MCU は京都大学からも提供しているが、大学間の MCU 共同利用に向けて他大学からも御提供頂けるようであれば大歓迎なので、是非ともご連絡頂きたい。また、高機能化に向けての要望もあればお寄せ頂きたい。

FaMCUs は国立情報学研究所の公式サービスではないため、十分なサポートを提供する体制を持たないが、将来に向けて、サポートや保守にかかる費用を大学間で分担しながらシステムが維持できる安定運用のための仕組みについても検討していきたい。

謝辞 FaMCUs, Vidyo ゲートウェイサービス, Skype ゲートウェイサービスの構築にあたりご協力頂いた (株) アットウェア, (株) 東和エンジニアリング, (株) ネットワークバリューコンポネンツ, Vidyo Japan (株), マッキーソフト (株) 各社の方々に、謹んで感謝の意を表する。

参考文献

- 1) Recommendation H.323, ITU-T.
<http://www.itu.int/rec/T-REC-H.323/e> (参照 2014 年 1 月 20 日)
- 2) S. Cantor, J. Kemp, R. Philpott, and E. Maler ed.: Security Assertion Markup Language (SAML) V2.0, 2005/3.
<http://saml.xml.org/saml-specifications> (参照 2014 年 1 月 20 日)
- 3) 山地一禎, 片岡俊幸, 中村素典, 曾根原登: シボレスシステムを用いた属性連携基盤の開発, 情報処理学会 研究報告 Vol.2009-FI-96, No.10, pp.1-8, (第 96 回情報学基礎研究会/第 37 回デジタル図書館ワークショップ) 2009/11.
- 4) 西村健, 中村素典, 山地一禎, 大谷誠, 岡部寿男, 曾根原登: 日本における学術認証フェデレーションとその役割および効果, 信

学技法, Vol. 111 No. 375, IA2011-55 pp.5-8, 2012/1.

5) 中村素典, 山地一禎, 片岡俊幸, 岡部寿男, 曾根原登: 学術認証フェデレーションにおけるテレビ会議用 MCU サービスの試験実装, 電子情報通信学会 2010 年総合大会通信講演論文集 2, pp. S130-131 (BS-7-6), 2010/3.

6) 学認技術運用基準, 国立情報学研究所 学術認証運営委員会, 2013/10/17.

<http://id.nii.ac.jp/1149/00000212/> (参照 2014 年 1 月 20 日)

7) 中村素典, 大川恵子, 工藤紀篤, 堀場勝広, 前田香織, 河野英太郎, 石野正英, 畠中翔, 八木啓介: 高品質映像による 4 地点インタラクティブ・リアルタイム講義の運営, ADVNET2007 広帯域ネットワーク利用に関するワークショップ, 2007/1.

8) J. Rosenberg, et al.: SIP: Session Initiation Protocol, RFC 3261, The Internet Society, 2002/6.

9) Codian Remote Management API Document Version 5, Tandberg, 2010/4.

10) Polycom RMX 1500/2000/4000 XML API Overview Version 7.6, Polycom, 2011.