平成 20 年度 情報処理軽井沢セミナーレポート

総合研究大学院大学　葉山情報ネットワークセンター　洞田　慎一

１．タイトル

「認証」と「認可」の連携 - UPKI を利用した総研大・基盤機関連携について-

２．概要

総合研究大学院大学は、国立情報学研究所などの共同利用研究機関を基盤研究機関として連携し、教育・研究・事務といった大学の機能を果たしています。一つ一つのキャンパスは、人数の規模では決して大きくはないものの幅広い専門分野をカバーしています。

この広範囲の教育・研究の規模を持続・発展させていくためには、それぞれのキャンパスが機能を継続的に発揮する面と、大学全体として各基盤研究機関と共同し全学的に機能を発揮する二つの側面が必要不可欠です。後者のような全学的な問題に対しては、ネットワークサービスが重要な連携の基盤となり得ると考えます。しかしながら、各基盤研究機関の特徴や背景、考え方などが異なるだけではなく、ネットワークシステムも必ずしも連携を目指して設計・運用されているわけではないため、全学的な連携が困難となる場合もあります。例えば、キャンパスを相互に往来した場合などネットワークやサーバ・サービス等へのアクセス権限について、利用資格が不透明なままネットワークサービスを提供、あるいは提供できていないことがあります。ネットワークサービスを全学的な連携の基盤とするにあたり、①ネットワーク担当者の連携や相互理解、②構成員の利用資格の相互照会及び認証と、それに伴うネットワークサービスの全学化が必要と考えます。

本案は、特に②の利用資格の相互認証について、機密性や完全性の機能保持に優れる PKI 基盤を全学的に整備し、電子証明書により利用者情報を運搬することで、利用者がキャンパスによらず適切なサービスを安全に受けることを可能とする基盤を構築することを考察します。利用者情報の照会や認証機能を全学的にサービスし、システムやネットワークへの利用資格の提供を行います。それぞれの基盤研究機関での既設のレポジトリサーバなどへ登録や照会を委任することで、ネットワーク管理者の運用コストの分散や、不明な利用資格者を分離などリスクの軽減が期待できると考えます。ネットワークサービスの基盤である認証や照会のしくみを整備することで、各基盤研究機関の特徴あるサービスや情報を共有・連携し、本学の全学的な連携の基盤へと発展させることが可能と考えます。

このような認証と認可の連携について、類似するものとして、セミナーにて説明がなされた EduRoam やグリッドであると考えます。セミナーで得た PKI を利用したこれらの連携サービスについての実現の方法や課題の説明を基に、前述した②の計画について、問題の背景と、実現に向けて必要な項目をまとめ、セミナー最終日に発表し、その内容を本レポートとしてまとめます。

３．セミナーで学んだ技術及び知識

（１）学内認証局の構築・運用にむけて ～概要および基礎知識～

CSI(サイバーサイエンスインフラストラクチャ)に関して目的や体制、効果について説明を受けた。UPKI による電子証明書基盤の構築が、CSI において重要な役割を担っていることや、連携(Federetion)の強化がキーワードであることの認識を深めた。実例として、EduRoam について説明を受け、実際に導入した場合の課題点などを認識した。また、PKI 構築において必要とされる CA や、証明書、運用のコストなど基礎知識として重要な内容を再認識することができた。

（２）UPKI 共通仕様の活用について ～CP/CPS ガイドライン詳細解説～

すでに、NII/SINET の説明会において、CP/CPS ガイドラインについて説明を受けていたが理解が十分ではなかったことを、セミナーでの説明から再認識した。すでに CA や証明書を運用している場合では、実際に発行する証明書や用途、手順を明文化することが、CP/CPS を規定することになることを理解し、CP/CPS ガイドラインの実際の利用方法を理解することができた。

（３）認証局構築実習

NaregiCA を学内にて運用していたため、導入までの問題点や困難性はある程度理解していた。実際の印象として、実際に機能させるまでに設定や調整など若干の困難性はあるもののその解決の方法は決して突飛なものや、特殊な知識を必要とするものではないため、一度インストール手段を検証すれば、運用機でのインストールはさほど難しくはないものと認識している。実習にてインストールしたサーバにおいて、証明書発行から失効まで一通りの機能を有効にすることが可能であったが、カードリーダライタとの相性の問題のため、IC カードへの書き込みはできなかった。逆に言えば、大学にて IC カードを使用した場合に、IC カードやリーダ、ライタなどの物理的なインターフェースについて有効に運用維持できるように保守に力を注ぐか、IC カードの運用をアウトソースすることで品質の維持を図るなどの方策が必要と認識し、PKI の構築以上にアプリケーションや物理的、環境的な整備にも注意を払う必要性を改めて認識した。

（４）認証局を実際に運用するには？

CA を実際に運用するにあたり、技術、制度、人など、運用や構築について様々な注意点の説明を受け、改めて実際に導入した CA について、設定等の見直しの必要性を実感した。特に PKI を構築するにあたり、技術よりも制度を整備することが重要であることを理解した点は大きいと認識している。また、大学間連携などのように、組織を超えた運用を行う場合、CP/CPS をもとにどのように照合しあうか、実際に NII にて監査という方式にてどのように担保しているのかを説明を受け、その重要性を再認識した。

（5）グリッドの認証と CSI の活用

グリッドのそれぞれの機能について、特に認証の部分について、まとまった説明を受ける機会がそれほどなかったことから、講義にて説明を受けた内容は、連携のために PKI がどのように活用され、グリッドでどのように応用や修正を施したのかが理解でき、グリッドでの利用以外でも有効に活用できる部分を多く認識した。

他の基盤研究機関では、実際にグリッドサービスを提供している（あるいは提供を準備している）研究所もみられることから、大学全体の問題としてどのように考え、UPKI をどのように活用するかをあらかじめ考えておく必要性を実感した。

４．セミナーを通じての成果

セミナーでの内容から、PKI を実現し、実際に他機関、他大学と連携するにあたり、技術よりも制度や、運用、継続性といった問題が非常に重要であることを改めて認識した。CA をそれぞれの機関にて運用することは実際には困難であろうということは実習からも感じ、実際の導入の現場では、PKI の構築に高い技術やハードルを感じられる場合が多いと考える。しかしながら、PKI の利用の際には、PKI 構築に用いた技術とは異なり、十分に運用できるレベルの知識や技術で運用でき、証明書の利用も、あまり利用者の目の見えない部分で（たとえば単純なアプリケーションサーバとは異なり）その役割を果たしているため、PKI 敷設後の運用は安易に扱われやすくなる可能性もある。連携した場合の相互の確認など、PKI を敷くために用いた技術よりも、実際に利用するのに必要な制度や管理・運用ルールを明確にしなければ、PKI 環境を維持できないため、その照合や評価の方法を含め、制度をどのように整備するかが課題であることを認識した。

このことは最終日の発表に内容になって現れ、事前課題の計画について、実現をするためには、制度や運用ルール、継続性を慎重に扱うべきとの結論にあらわれている。

５．セミナーの事前、事後において、参考になった URL とその簡単な内容紹介

PKI については、複数の参考書があるため、それぞれを列挙することはできないが、いくつかの資料を集めた際、「PKI の概念についての説明」に焦点をあてているもの、「PKI の構築や証明書の利用、CA の運用の仕方」や「VPN、シングルサインオンなどの応用機能」を中心に扱うもの、「システム監査など、制度やルールについて」焦点をあてているものが見られた。それぞれ参考にする際には、何を必要としていて、どのような目的で運用をスタートしたいのかに大きく依存するものと考えられるが、概念に触れるのと同時に、箱庭のような、閉じた小さなネットワークの中で、実際に実証しながら進めると理解や、CA の選定に有効ではないかと感じている。実際に、CA を構築するに当たって集めていたものとして、Windows Server Enterprise Edition での CA の運用の方法はマニュアルや参考書も多く、Windows Server での Active Directory 環境での閉じた運用であれば、効果や役割を理解することはさほど難しくはないと感じた。

６．事前準備として知っておいた方が良かったと思われること

UPKI や SINET などの説明会での資料収集や動向調査が必須と思います。また、IC カードの導入などを目指す場合、やりたいことの把握と、ニーズの把握、先行大学での問題点の把握など、事前課題を通して見えてくるであろう問題を把握しておくのが望ましいと思います。

また、セミナーハウスの設備内容や、ネットワーク環境や（おそらく参加者のほとんどはなにかしらの業務を抱えたままセミナーに参加していると思いますので）VPN などの接続要件の確認をあらかじめ事前にしておいた方が無難です。

７．セミナーの感想等

少人数で、まとまった期間にてセミナーを受講できるため、大人数での説明会よりも多くの情報を集中して聞くことができ、質問を通して細部まで尋ねることができるため、説明会に参加して、セミナーを受けていると、より理解が深まると思いました。

また、食事や、休憩時間を通して、講師やスタッフの方々、他の参加者らと交流し情報を交換できる時間も多く、講義以外で受け取ることができる情報も多くあります。

大変有意義なセミナーであったと実感しております。セミナーを快適に過ごせるように御配慮いただきましたスタッフの方々に御礼申し上げます。

「認証」と「認可」の連携
- UPKIを利用した総研大・基盤機関連携について-

平成20年度情報処理軽井沢セミナー　自由演習課題
/ 2008.09.05於　国立情報学研究所軽井沢国際高等セミナーハウス

国立大学法人総合研究大学院大学
葉山情報ネットワークセンター
洞田　慎一

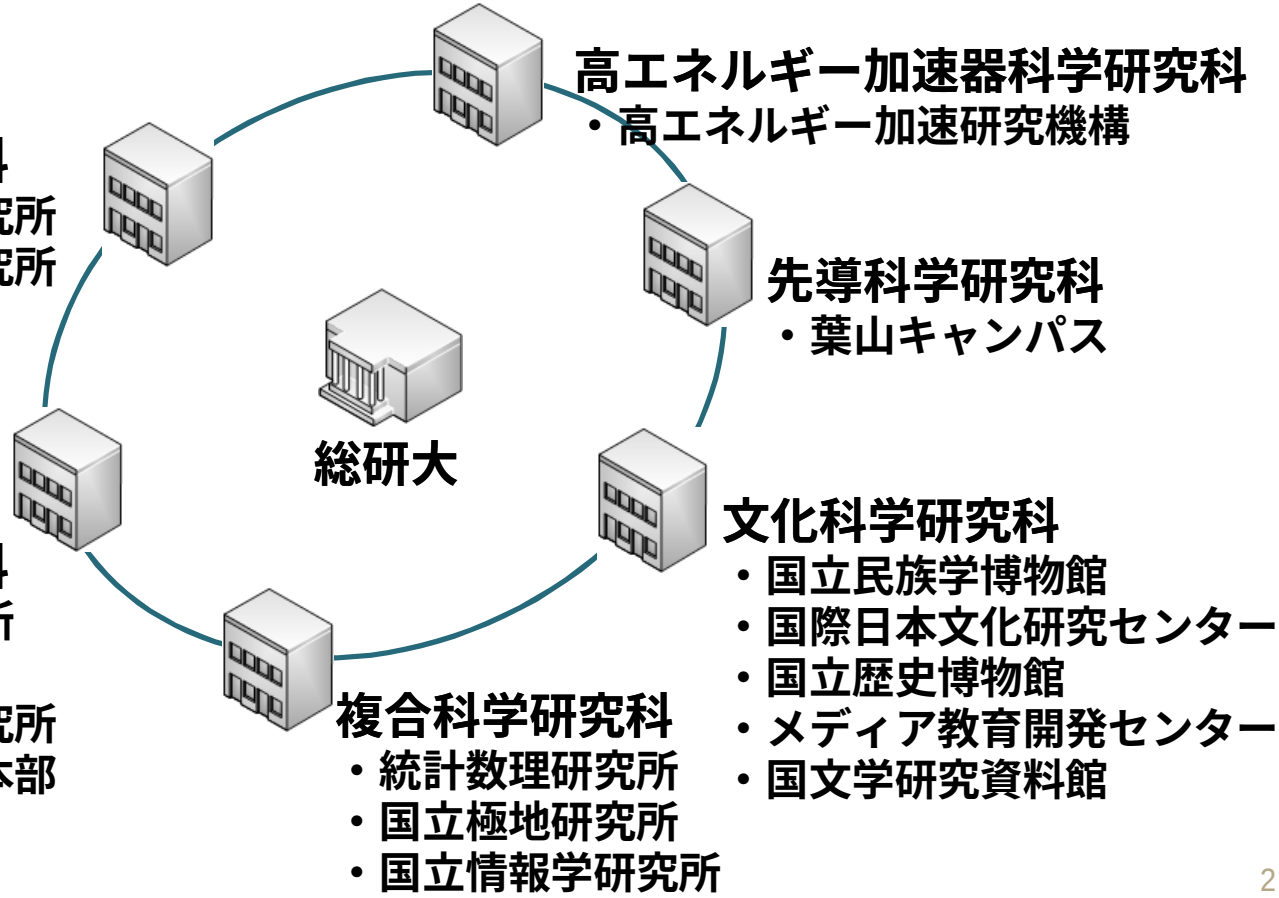
1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

セミナーで改めて実感したもの

「連携」に必要なのは、「技術」ではない。「人」や「制度」を予めどこまで考えておくか？どこまで突き合わすか？

1. 総研大について

【総合研究大学院大学】
・博士課程（5年あるいは3年）の大学院大学です。
・国立情報学研究所や国文学研究資料館など、全国各地の共同利用研究所を基盤研究機関として連携し、それぞれがキャンパスとして教育・研究の場となっています。
・活動内容、場所、時間、すべてが広範囲に拡がっています。



1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

総研大を説明すると、「連携」という言葉を使うことが一般的かと思います。

↓

実際には、それほど容易ではなく、うまく調整できないこともよくみられる。

■　例えばネットワークに関する問題点

・基盤研究機関をそれぞれ行き来した場合のネットワークやサービスの基本方針の差
（それぞれの機関でポリシーや手順が異なる）

・それぞれをつないだ全学的なシステムなどを設計、運用する場合の連携、調整

↓

連携を困難にしているのは・・・
- 人的な問題（連携、調整の不足）
- 制度的な問題（ポリシー、手順の差）
- 技術的な問題（連携考慮・最適化するよう設計されていない）

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

連携は総研大では生命線

教育　最高最大レベルの研究の場の提供。理系から文系までの幅の広い研究分野を教育可能にする。

研究　セミナーで取りあげられたグリッドもそのような例の一つと認識

事務　機関間の連携は、同一大学での遠隔地のキャンパスでの連携というよりも、他大学との連携に近い。

遠隔地なのだから、ネットワークに追ってくる部分は大きいと認識

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

■「連携が進まないことの原因」に対処するために

ー事前課題での計画案ー

①　ネットワーク担当者間での連携の強化

- SWS（共同利用機関におけるセキュリティーワークショップ）
- 各基盤研究機関のネットワーク管理部局へのアンケート

総研大関係の構成員
高エネ、岡崎、天文台、核融、国文研、日文研、葉山

②　「制度」と「技術」への対処
UPKIやShibbolethによる連携を目指した仕組みの可能性
ユーザや情報の管理をそれぞれで分担しながら緩やかに連携

2.葉山におけるNaregiCA

・NII/SINETでの説明会などでの情報を基に独自に導入
・導入当初より用途は定まっていた（認証ネットワークでの利用）
・しかし、独自で実装するよりも、連携や、今後の学内での証明書利用のシーンを想像し、まず準備を施した

何に使っているのか？

・学内認証ネットワークのEAP-TLS用証明書の発行
・SSL-VPN用の証明書発行
・学内サーバのクライアント認証の実証実験

何故、NaregiCAを選択したのか？

・UIやドキュメントが整備されており、実務利用が耐えられるフリーのCA管理ソフトウェアであること
・OSやクライアントのブラウザなど処理環境にできるかぎり依存しないこと（OpenSSLでCSRを作って、という運用ができること）

どのように運用しているのか？

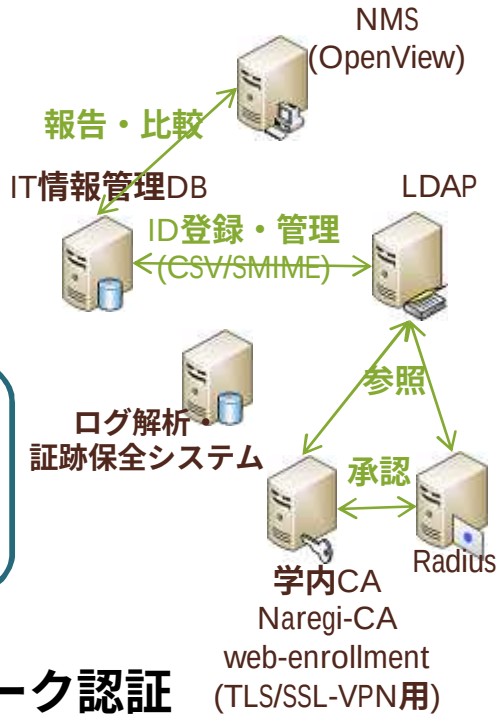
・３名がRAOperatorの鍵を所有（うち２名は事務職員）
・それぞれで、発行できる証明書の種類を分離
・発行と再発行の操作の説明は、さほど日数を要しなかった

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

葉山の認証ネットワーク・・マルチプルサプリカント＋動的VLAN

■　事務局ネットワークの認証方式

- IEEE802.1x(EAP-TLS)による証明書ベースの認証
- 教育研究や一時利用者からの明確な利用者の分離を目指す



- 証明書を作る
- PCにインストールする

→ パソコンを本人に渡す

知らないPCは事務ネットワークには入らない

利用者には、このしくみや証明書の利用をネットワーク認証での利用以外に説明をしているわけではない。

↓

もし、利用者から「これやりたい」と言われたら・・・

「PKIでできるよ。しかももうできてるよ」と答えることが可能

プライベートCAでは、「CAの鍵」と、「本人の証明書」を、明示的にインストールしてもらうには、「目的」で進めたら説明することが多すぎる。

「PKI？それどこのICカード？など、利用者の理解は短時間には進まない

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

３．基盤連携では？

NaregiCAを考えた先には、UPKIもあった

・情報研、高エネ研はセミナーで説明があったEduRoamに対応している。
・ネットワーク利用に認証機能を用いている機関も多い。

機関を移動した場合や、それぞれのサービス連携を考えた場合、機関・利用者へそれぞれ分担が必要になりつつある。

基盤連携を進る上で、各機関で担当する役割や分担、手順などをあきらかにしていく必要もある。

■ 原点としては・・・

基盤連携の際に、必要なのは、「どこ」の「誰」なのか？という情報がもっとも必要か？

- ID、パスワードを持っているから、「その所属の人」と判断するのは問題であろう
- PKIを用いた場合、暗号化、というよりも本人性確認が強力
- 証明書の発行や管理(RA)は、各機関に分担を依頼することは、まだ可能ではないだろうか？
- しかしながら、各機関の制度、ポリシー、手順に大きく依存

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

■　連携の基本レイヤは、信頼関係か？

・素朴には、基盤連携は、ほとんど「認証」と「認可」をどう規定するか？という部分がほとんどを占めているのではないか？
・セミナーでのグリッドによるPKIの説明についても、「認証」や「認可」に関する部分は、特に様々なしくみが施されていることの説明を受けた。

結局、利用者が使いたいサービスやサーバは、「認証」と「認可」の後に提供されるからであろう。

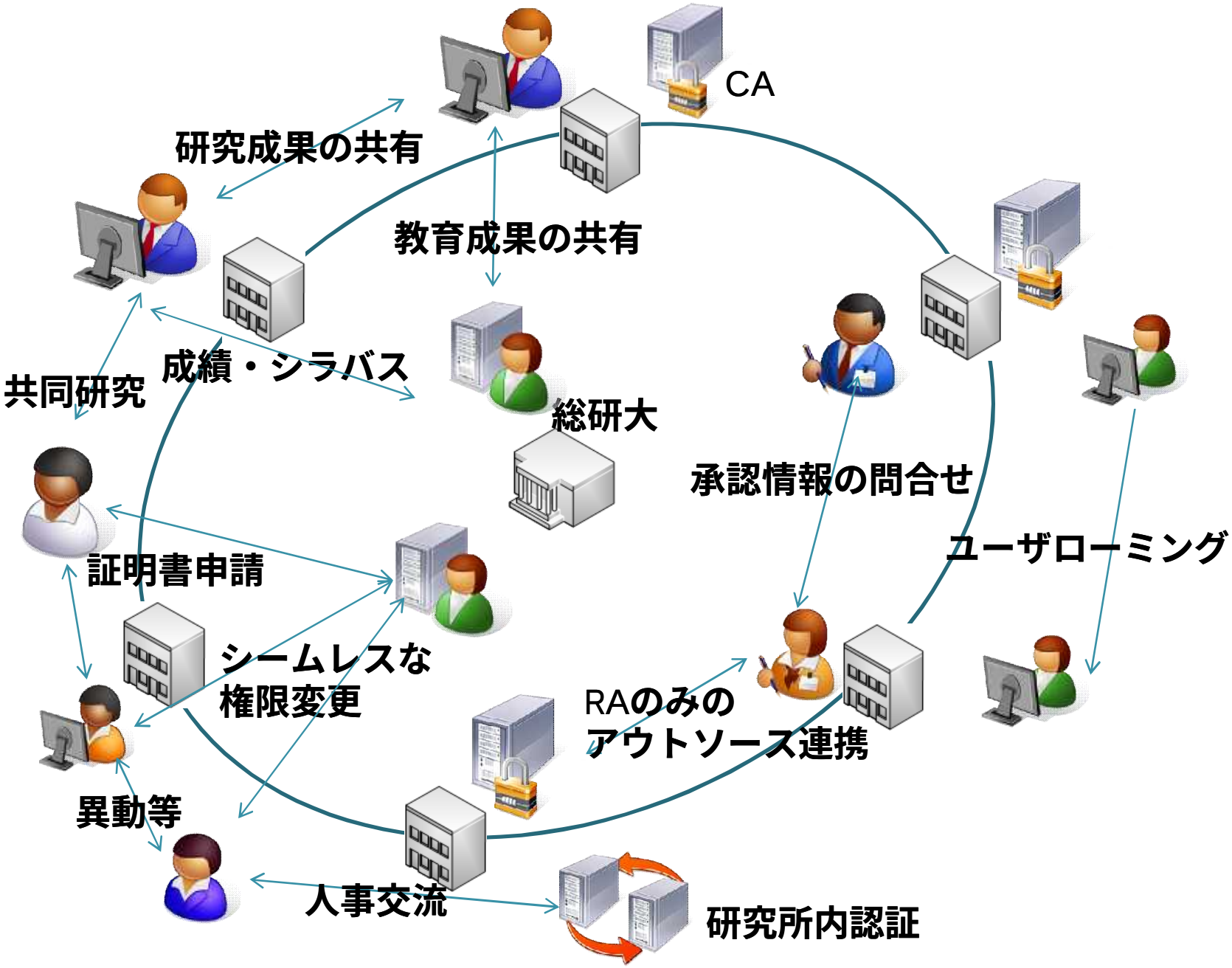
■　しかしながら、PKIで処理可能かはアプリケーションや環境に依存

- IDとパスワードという素朴な方法も確保しておくべきだろう。
  というよりも、PKIでの自動的な認証は、証明書の譲与など、運用は危険を伴う可能性がある。
- ２ファクタ認証という枠組みをうまく利用してみる。
  PKIは本人確認にしか使わない場合もありうるのではないか。

・　現時点では、UPKI+Shibboleth（あるいはSAMLやリバースプロキシ）のようなものが、現実的か？
・　しなしながら、現実のサービスでは各基盤機関での事情を考慮して進める必要性がある。

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

連携のイメージ・・・「連携の潤滑油としてのUPKI」



1.総研大

2.葉山CA

3.基盤連携

4.効果

5.まとめ

４．効果とリスク

- **連携に一歩前進できるだろう**
  基盤間の交流は、教育・研究に効果や期待が大きい
- **互いの特徴あるサービスの共有**
  基盤機関で独自に熟成された特徴あるサービスを全学的に共有
- **作業を分担して運用コストとリスクを分散**
  作業や負担をいたずらに増やすことなく、運用にかかるコストやリスクを分散しないと持続できない。
  セミナーでは、技術よりも継続性が重要であることが説明された。
- **サービスが停止した場合**
  復旧時間は限りなく０が期待されるであろう。
  つまり連携の心臓部にかかるシステムは無停止でなければならないだろう。
- **お互いの信頼性の確保**
  UPKIでの連携についてもCP/CPSの内容からお互いの信頼性をどのように確保するかが課題となっていた。
- **ユーザのリテラシの問題**
  ユーザはそれぞれスキルや考え方が違い、理解には時間がかかる。ユーザの環境をなんら変更せず、透過的なレイヤーであるのが望ましい。

5. まとめ

- **実現可能か？**

  技術的には実現困難というわけではないが、人や制度に関するリスクにどのように対処するかが肝要
- **問題の一つは制度**

  ポリシ、手順、CPSなど規程類を基盤間でどのように照合・評価するか？
- **人や予算を新たに充填せずに可能か？**

  利用者も管理者も今のスタイル、ワークフローを大きく変えずにシームレスに連携・運用できなければ持続は難しい。

実現にむけて・・・

- まずCP/CPSを、センター内規・申し合わせとして策定する。
- 話し合いの機会を持てるよう検討する。
  - SWS(全国共同利用機関セキュリティーワークショップ）など

■　最後の結論は、PKIともCAとも関係が薄れつつありますが、それだけPKIが強力な基盤であるため、「人」と「制度」をどうやってコントロールし、内容を網羅しておくか、という点が重要であるという、このセミナーで得た成果であった所以だろうと思います。

講師の先生方、スタッフの皆様、また共に受講した皆様に感謝いたします。

1.総研大
2.葉山CA
3.基盤連携
4.効果
5.まとめ

国立大学法人
総合研究大学院大学
葉山情報ネットワークセンター