「認証」と「認可」の連携
- 押し付け合いではない総研大・基盤機関連携 -

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

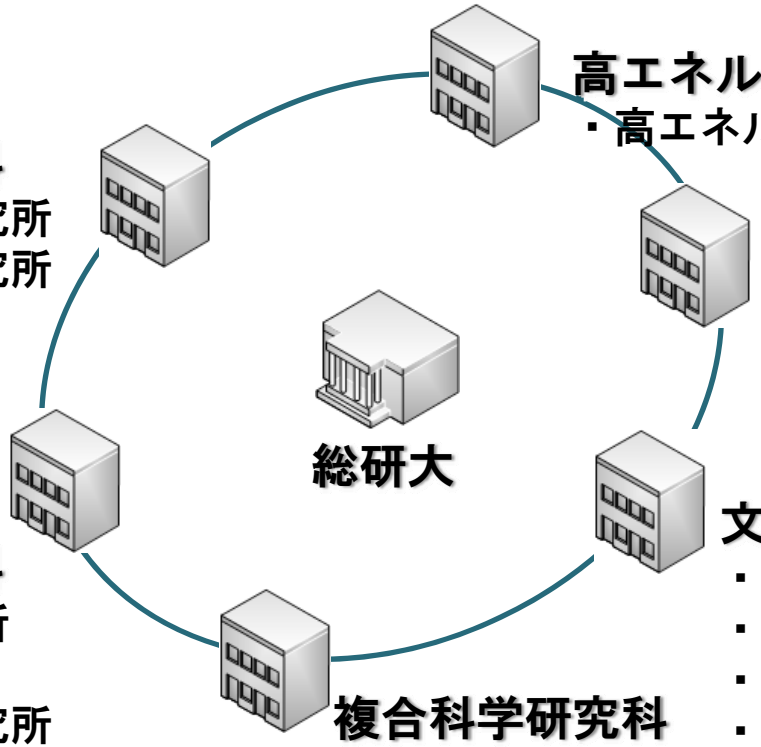
1.総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

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。



高エネルギー加速器科学研究科
・高エネルギー加速研究機構

先導科学研究科
・葉山キャンパス

文化科学研究科
・国立民族学博物館
・国際日本文化研究センター
・国立歴史博物館
・メディア教育開発センター
・国文学研究資料館

複合科学研究科
・統計数理研究所
・国立極地研究所
・国立情報学研究所

物理科学研究科
・分子科学研究所
・国立天文台
・核融合科学研究所
・宇宙科学研究本部

生命科学研究科
・国立遺伝学研究所
・基礎生物学研究所
・生理学研究所

1. 総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

総研大の説明をすると、「連携」なんて素敵な（？）言葉がたくさん繰り返されますが・・・

↓

実情は「KY」

＊おそらく＊、お互いに「知らない」、「知らなくても済んできた」という状況があった。

■　それでも歯車は動く（研究会、セミナー、人事異動など）

・分からなくても相談もなく勝手に使う。

・で、勝手に問題を起こしてくる。

「私は、〇×研の教授だ。だから使わせろ」

「△□研では使えた。だから使わせろ。直せ」

「〇△館と事務連携したい。だから使わせろ。作れ」

「△×館ではポリシを作った。
でもPCを亡くしたのは総研大の学生だ。総研大で考えろ」

「知らないってば」
で、どうしろと？

連携を妨げている最大の障壁は・・・「人」と「無知」と「押し付け合い」

連携は、たぶん総研大では生命線　・・・　機器感は有って無いけど

教育

「総研大として入ったのに、すべて誇大広告」（学生談）
学生が望んでいるのは、最高最大レベルの研究の場。

研究

グリッドもそのような例の一つ。そもそも共同利用研。
独自で閉じていいものでもない。

事務

例えば学務・基盤連携、その他大学に必要な事務機能
はほとんど欠落。成績や単位、シラバスもすべて紙

遠隔地なのだから、ネットワークしか、ないのだろうねぇ・・・

1.総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

■「連携が進まないことの原因」は「人と無知」、対処できる？

① お互いにもうちょっと交流しようよ

SWS2007
第11回 共同利用機関におけるセキュリティワークショップ

総研大関係の構成員
高エネ、岡崎、天文台、核融、葉山

今年（SWS2008）は岡崎自然科学研究機構で開催（9月29日、30日）
各基盤研究機関のネットワーク管理部局にアンケートを出してみた。

② 制度と実装で自由度をコントロールしてみようよ
UPKIとかShibbolethとか使えないか？
ユーザ管理は分担しようよ。

2.葉山におけるNaregiCA

・独自に入れましたが、苦労しただけの価値はあると思っています。
・用途は決まっていましたが、「大きな構想より、先に先手を打って、余計なシステム導入をやめさせる」方が先決
（再び「失われた１０年」に戻ってしまうので）

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
SSLVPN用の証明書発行
第４種おれおれ証明書の無制限発行機

どうしてNaregiCAなのか？

大前提・・・証明書発行にお金はかけたくない（かけられない）
Webでいいから、コマンド以外のUIが使えること
日本語UIであること・・・運用は事務局担当者
できれば、OpenSSLでCSRを作って・・・という運用ができること

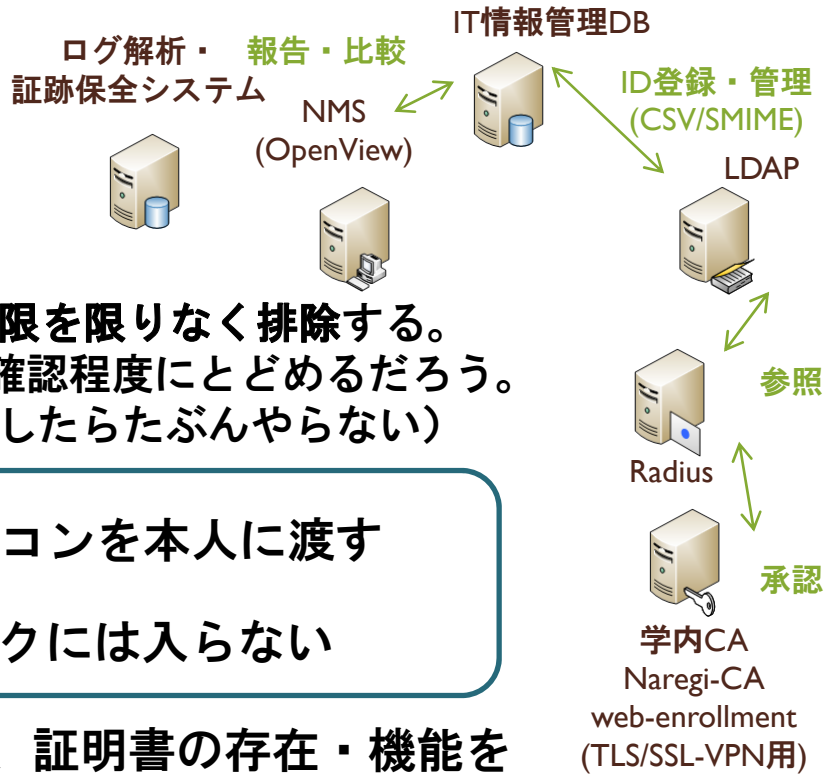
どれくらいのコストで運用しているの？

自分を含めて３名がRAOperatorの鍵を持っています。
自分はEAP-TLS用証明書の証明書は発行できません。
（事務局PCに使う証明書なので）
発行と再発行の操作を１０分くらい実演したら覚えてくれました。

1.総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

葉山の認証ネットワーク
有線、無線ともマルチプルサプリカント＋動的VLAN

教職員と一時利用者は、MACアドレス認証あるいは、Web認証。つまり、お宝は事務局という考え。



※葉山のポリシは、**教員から直接操作の権限を限りなく排除**する。
たぶんSSOしても、できることは予算額の確認程度にとどめるだろう。
（紙で書くと自分で確認するけど、電子化したらたぶんやらない）

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

でも、利用者たちには、この仕込みや、証明書の存在・機能を教えていない。でも、管理者の一部は将来像を共有

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」と答えられる。

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増えすぎる。

「PKI？それどこのグループウェア？とか、結局はわかってもらえない」

1.総研大
2.葉山CA
3.基盤連携
4.リスク
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、高エネ研はすでにEduRoamに対応している・・・
岡崎はネットワーク利用に申請と審査を義務付けた

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、期間・利用者への権利や責任、義務に対して、応分の分担が必要になりつつある。

基盤連携を確立させるには、たぶん、それぞれの機関に責任を自覚させた方がよいかもしれない。

■ 従来までの連携での産物は、ほぼ運用機関への丸投げ
あまり手続きや方法論は参考にできないだろう。

■ 原点・原理としては・・・
たぶん、基盤連携した際に、必要なのは、「どこ」の「誰」なのか？

- ID、パスワードを持っているから、「その基盤の人」と判断するのは早計だろう？
- 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、各機関の仕事として自然にできるだろう。

（昇任人事等、葉山は何も聞いていません）

1.総研大
2.葉山CA
3.基盤連携
4.リスク
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といってもいいだろう。

なぜなら、利用者が使いたいサービスやサーバは、その行為の後についてくるから。

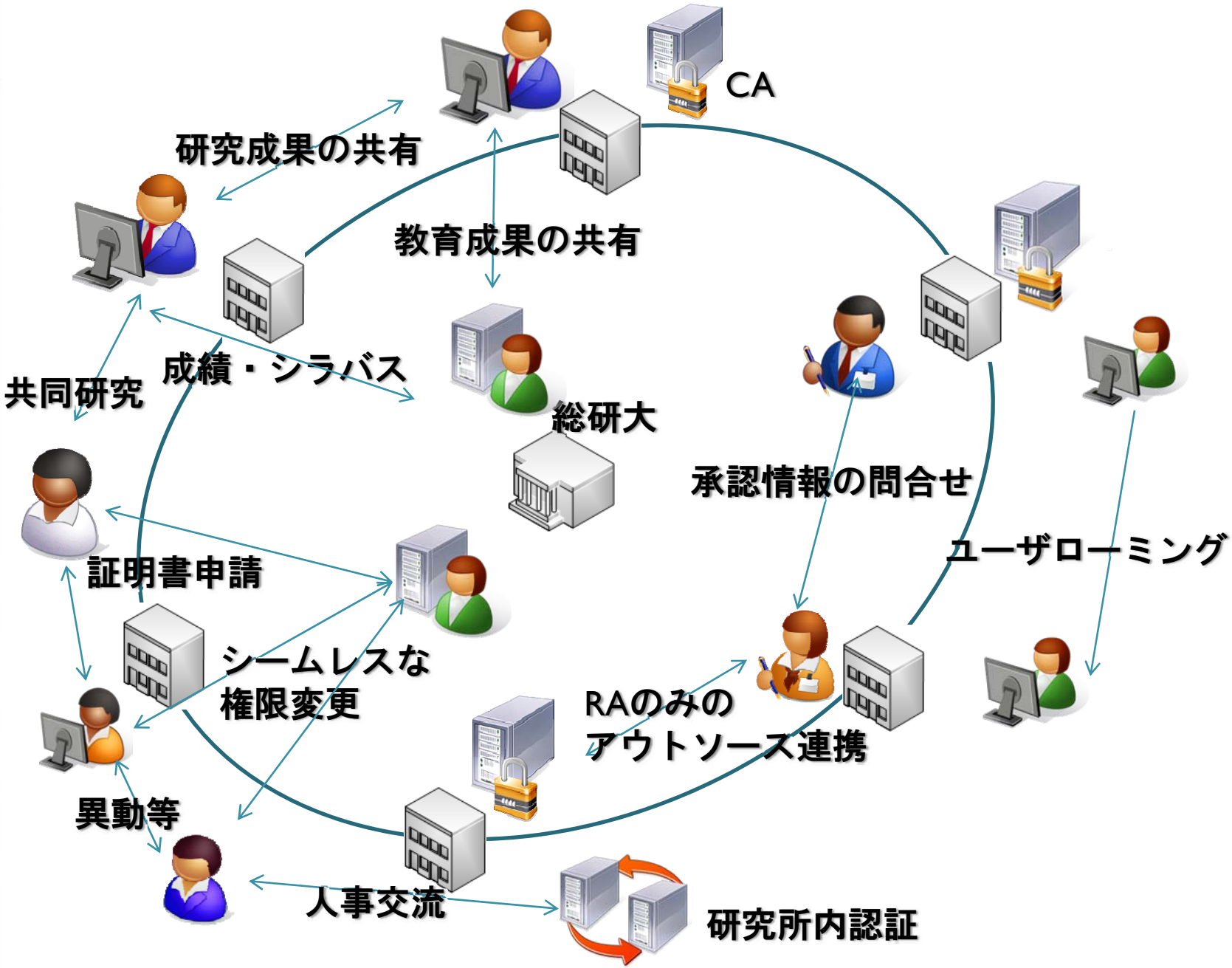
■　でも、PKIについてこれるかどうかは、アプリケーションや環境に依存

- 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、教員の運用はかなり危険を伴うだろう（学生に貸す）
- ２ファクタ認証などをうまく利用しておく。
  PKIはむしろおまけ（本人確認にしか使わない場合もありうる）

・　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？
・　ポータル、とすると多分基盤から反発を受ける（自前で持っているものがあるのに、何故さらに利用を増やすのか？）

1.総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

連携のイメージ・・・「連携の潤滑油・・・みたいな・・・」



1.総研大
2.葉山CA
3.基盤連携
4.リスク
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、研究においては効果や期待が大きい
- **不用意な新システムの開発防止**

  〇×先生の開発システム研究の中途半端な途上システムは嫌
- **作業を分担して運用コストとリスクを分散**

  「葉山」のことは「葉山」で、「基盤」のことは「基盤」で

  「ただ」ぐらいの価格で（必要経費分ぐらいで）、心の障壁なく運用し続けられる規模ぐらいに運用コストを分散しないと持続できない。
- **サービスがこけた場合**

  復旧時間はかぎりなく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**

  本当のところ、お互いに信頼しあえるのか？技術的にではなしに、概念、偉い人の性格、性質、考え方的に
- **ユーザのリテラシの問題**

  ユーザはたぶん理解しない。小人さんがなんかやってくれている的に、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。また、スキルや考え方も違う

5. まとめ

- **実現可能か？**

  リスクがあるから、効果も大きいわけで、やれない技術でもなければ、挑むのは、まあ妥当だろう。

- **問題の一つは制度**

  ポリシ、運用手順、CPSなど規程類を基盤間でどう照らし合わせられるのか？

- **人を新たにアサインできる余地はない**

  利用者も管理者も今のスタイルを変えずにシームレスに連携・運用できるか？持続できるか？

- **制度と人という問題は、トップダウン式が望ましいが・・・**

  おそらく、今の経営陣にその判断は無理。ボトムアップで何らかの成果が必要かもしれない。

- **監査というネバーエンディングな問題**

  監査協議会の話を聞く上では、機関を通じて会計監査ぐらいしか考えてもらえていないのが現状。むしろ運用側で相互に確認し、担保として、改めて外部監査に監査報告書を書いてもらう方がよいかもしれない。

1. 総研大
2.葉山CA
3.基盤連携
4.リスク
5.まとめ

実現にむけて・・・

- まずCP/CPSを、センター内規・申し合わせとしてつくる。
- とりあえず、SWS(全国共同利用研究機関セキュリティーワークショップ）で話し合ってみる
  - 今年度の検討項目
    - 総研大の他の基盤機関への呼びかけ
    - アンケートの実施と、基盤担当者の把握
    - 「情報リテラシ演習」のような基本的なマナーをどう講習するか？
    - 基盤間で共有できる「モノ」とはなんだろうか？

■　最後の結論は、なんらPKIともCAとも関係なくなってきていますが、それだけPKIが強力すぎるので、「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故だろうと思います。

講師の先生方、スタッフの皆様、また共に講義を受けた皆様に感謝いたします。
NaregiCAのインストールとカードリーダではまったことは忘れないでしょう。そしてたぶん、ICカードは買いません。

ご清聴どうもありがとうございます。