学認アンケート2015総評

トラスト作業部会　主査 佐藤周行 （東京大学）

@NII オープンフォーラム 2016

学認アンケート

- 2012年から開始して今年で4年目になります

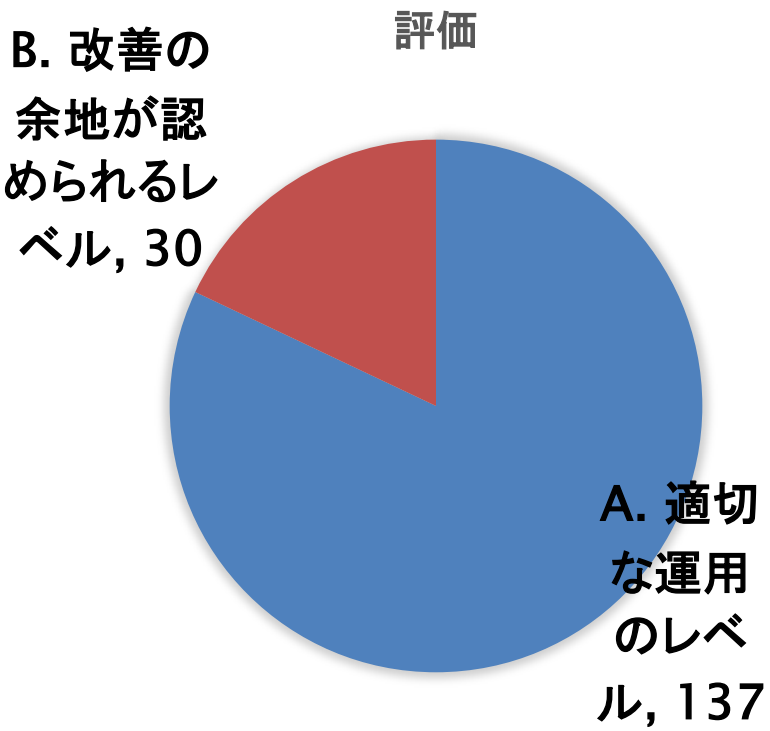
- 学認アンケートの目的:
  - 一義的には、学認参加組織が「実施要領」「技術基準」を遵守してIdPを運用しているかどうかの調査
  - IdPの運用管理を安定してできるようにするための、ポイントのガイド

- 対外的な主張:
  - 学認がトラストフレームワークとして機能し、参加組織がポリシーの下に正しく運用を行っていることのエビデンス(たとえ自己申告であっても)

2015年度の傾向

- 2014年度に参加組織が大幅に増えました（2013: 71, 2014: 136, 2015: 167）。2015年度はその2年目です。
- 以前から参加している組織についてはIdPの運用が安定してきたことがうかがえます
- （残念ながら過年度に改善をお願いした）組織の多くで改善が見られました
- 今年も改善をお願いした組織がいくつかあります（30機関）。引き続きの運用努力をお願いします

全体として



参加組織数　167
回答数　166

適切な運用　137
要改善　30

運用管理に気を付けるべきこと

- 学認アンケートの項目を分類し、どのような目的で項目が立てられているのかを見てみます

- 一般に「トラストフレームワーク」でのIdPの運用を考えるとき、ポリシー、統制で注目すべきは以下の3つ
  - Governance
  - Privacy
  - Technical

さらにドリルダウン

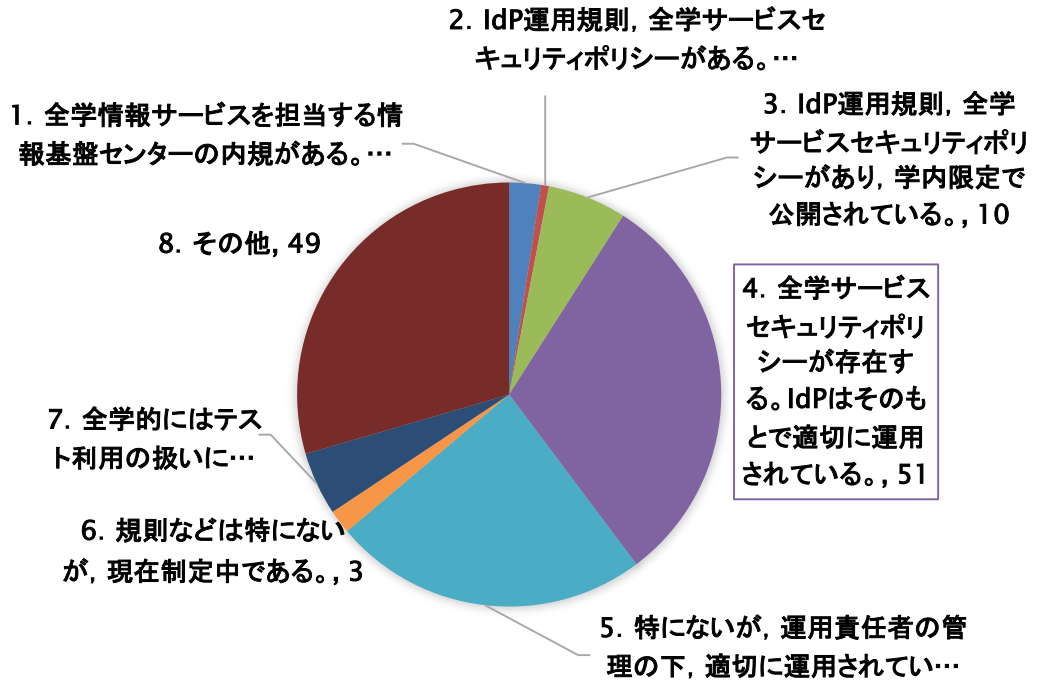
- Governance
  - 運用の統制。特に運用規則が定められているか
- Privacy
  - IdPのデータは適切に扱われているか
    - 特にUser Consent
- Technical
  - アイデンティティのライフサイクル管理は適切か（特に更新、廃棄）
  - クレデンシャルの管理は適切か
  - リモートの認証の手法は適切か
  - プロトコルは適切か
  - その他、一般的なシステムのセキュリティ

Governance

- 上位の規則があって、IdPの運用規則が定められていることが望ましい
  - セキュリティポリシーに関する「サンプル規定集」のうち、IdPに関する部分が新たに定められましたので参考にしてください

- IdPの運用規則が定められている組織 （徐々に改善されている）

  2014年度　47/136 → 2015年度　70/167



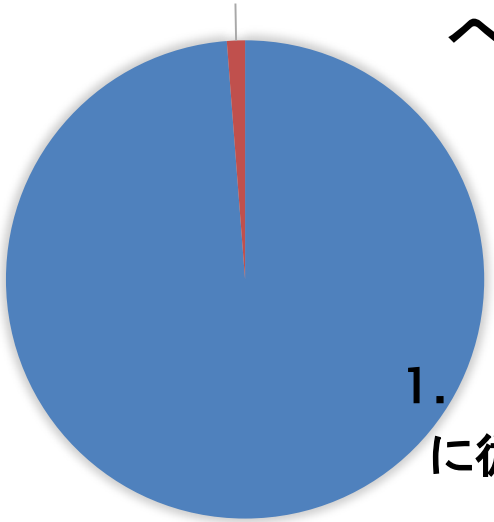
IdP運用上での根拠規則や内規の制定状況について

プライバシーについて

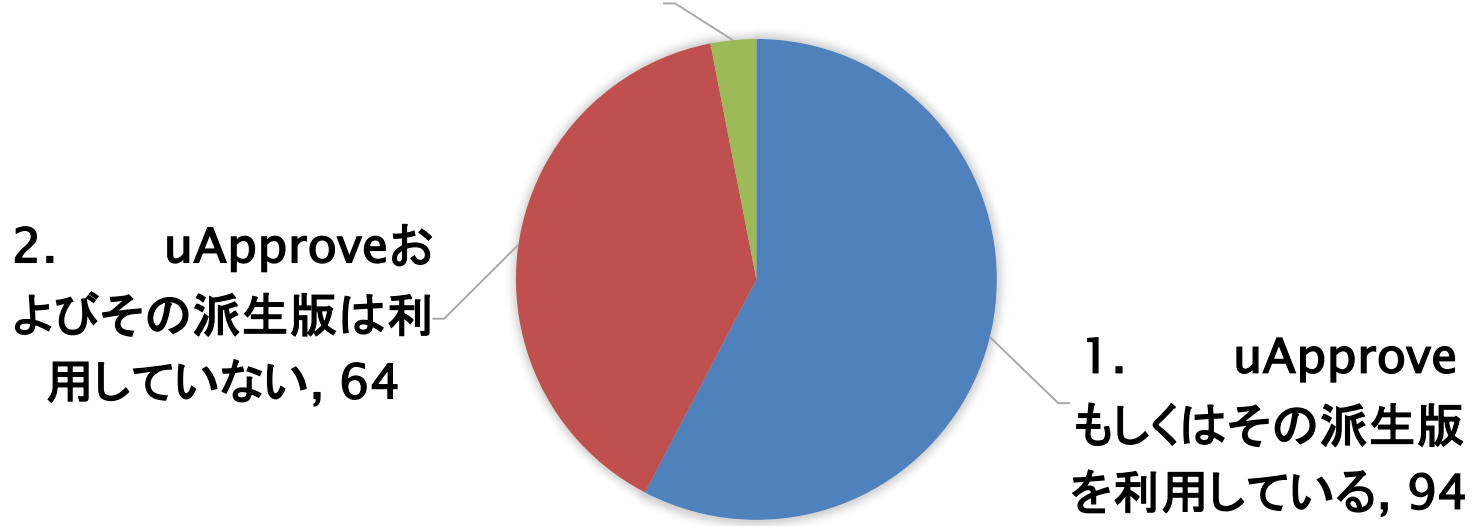
- 個人情報保護法群のうち、どれが適用されるかで若干異なるが「利用者同意」を得るのが基本形
- 数年前なら「注意深く運用」で対応できたものが、そうではなくなりつつある
- サービスの利用開始にあたって同意を取る（オンラインまたはオフライン）等の手段の検討が必要
- Shibbolethでは、V2ならuApprove, V3なら組み込みの機能で利用者同意を得る機能が提供されている

の導入率は前年より上昇していました。

個人情報保護に関する法令への遵守状況



利用者同意を得る方法


3. Shibboleth IdP Version3の属性リリース同意取得機能を使っている, 5
2. uApproveおよびその派生版は利用していない, 64
1. uApproveもしくはその派生版を利用している, 94

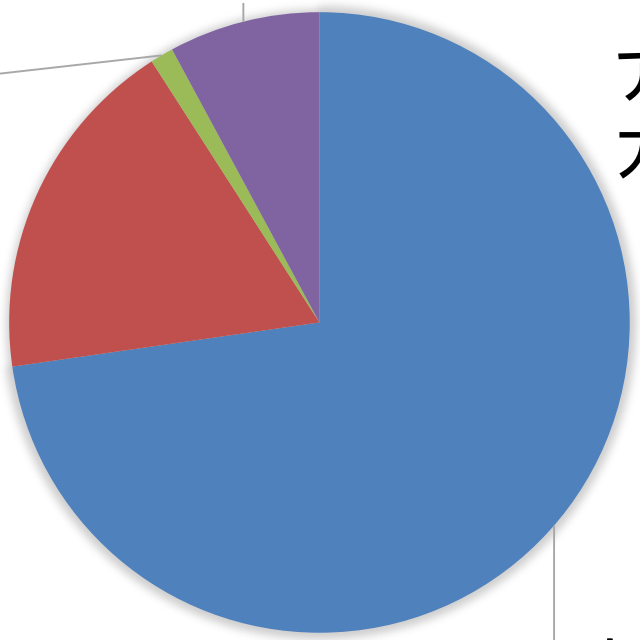
Technical

- 基本は、アカウント管理

- 組織の信頼のもとになる「Trusted DB」からアカウントが生成されているか
  - これをもとにしないと、アカウント数の増加、管理属性の複雑化等を考えると、管理のスケーラビリティを持たない方法では、早晩行き詰ることが予想される
  - Trusted DBと「直結」するには、業務フローや管理規則を整備することが必要

4.　その他，13

3.　利用者IDを作るときには，部局長印のある書類を提出し，管理者群がダブルチェックをしたうえで行っている。，2



アカウント作成の方法

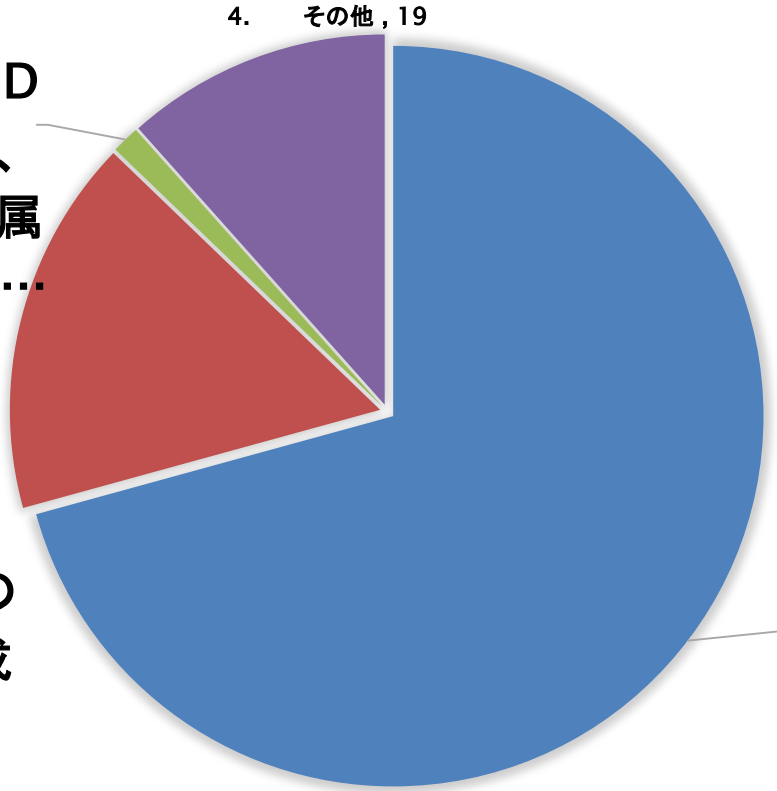
2.　利用者IDのデータベースは，Trusted DBから作られたものではないが，教職員や学生を直接把握している部局事務が責任を持って運用しているDBから作られてい…

1.　利用者IDのデータベースは，Trusted DBに基づいて作成されている。，120

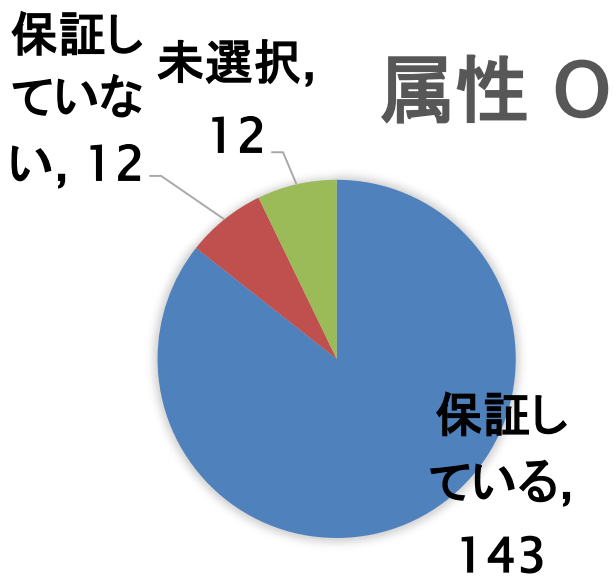
アカウント管理 → 属性値の保証

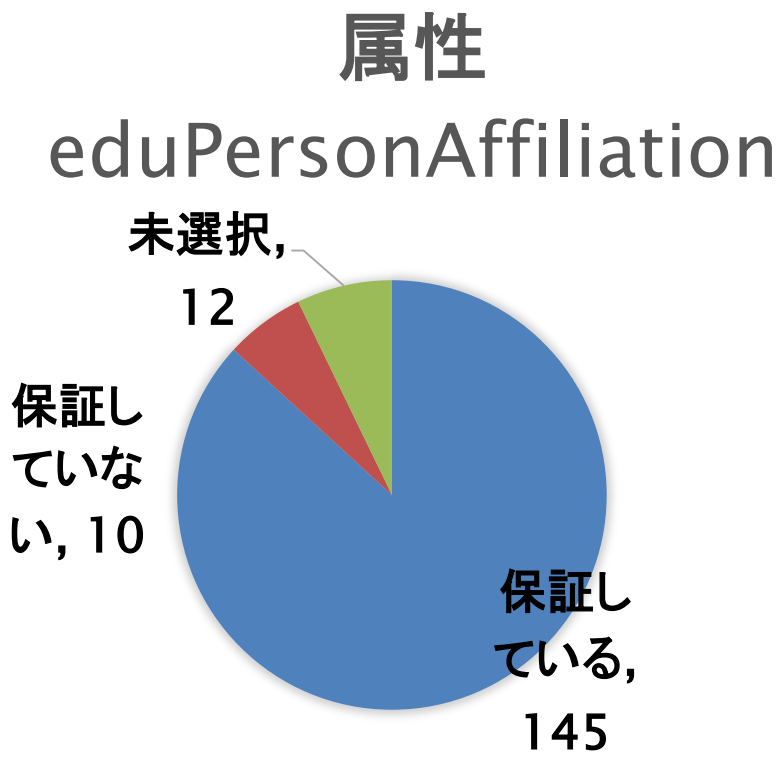
- 今回は、属性値の保証についても注目しました
  - システムのConfigが正しく管理されていれば属性値Oは、組織が保証できるはずです
  - アカウントがTrusted DBと直結して生成されているならば、属性値eduPersonAffiliationは、組織が保証できるはずです
  - 属性値は今後ますます重要になってきます。システムの構成管理を正しく行うことで正しい属性値の送出ができるシステムを運用することが望まれます

属性の計算方法


4. その他 , 19
3. 利用者IDの属性は全て、Trusted DBの属性から生成され…
2. 利用者IDの属性の一部には、Trusted DBの属性以外から生成されているものがある。, 27
1. 利用者IDの属性は、Trusted DBの属性のみから計算されている。,…

2つの属性


属性 O
保証していない, 12
未選択, 12
保証している, 143

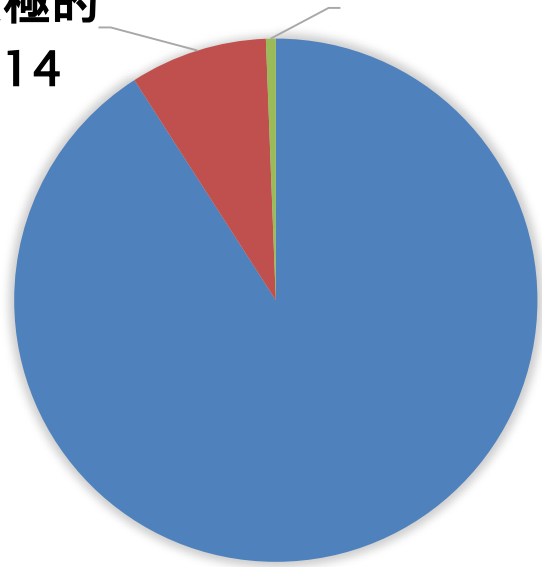

属性
eduPersonAffiliation
未選択, 12
保証していない, 10
保証している, 145

GakuNin

- クレデンシャル（ほとんどがパスワード）の管理
  - まだ（しばらくは）パスワードが主流という前提で
  - パスワードの管理は、パスワードポリシーによる管理と、パスワードに対する攻撃の周知、さらにパスワードが破られた時の被害の理解でおこなうしかありません
  - ほとんどの機関がパスワードポリシーを定めていました

2. パスワードポリシーは定めていないが，啓蒙活動を積極的に行っている。，14

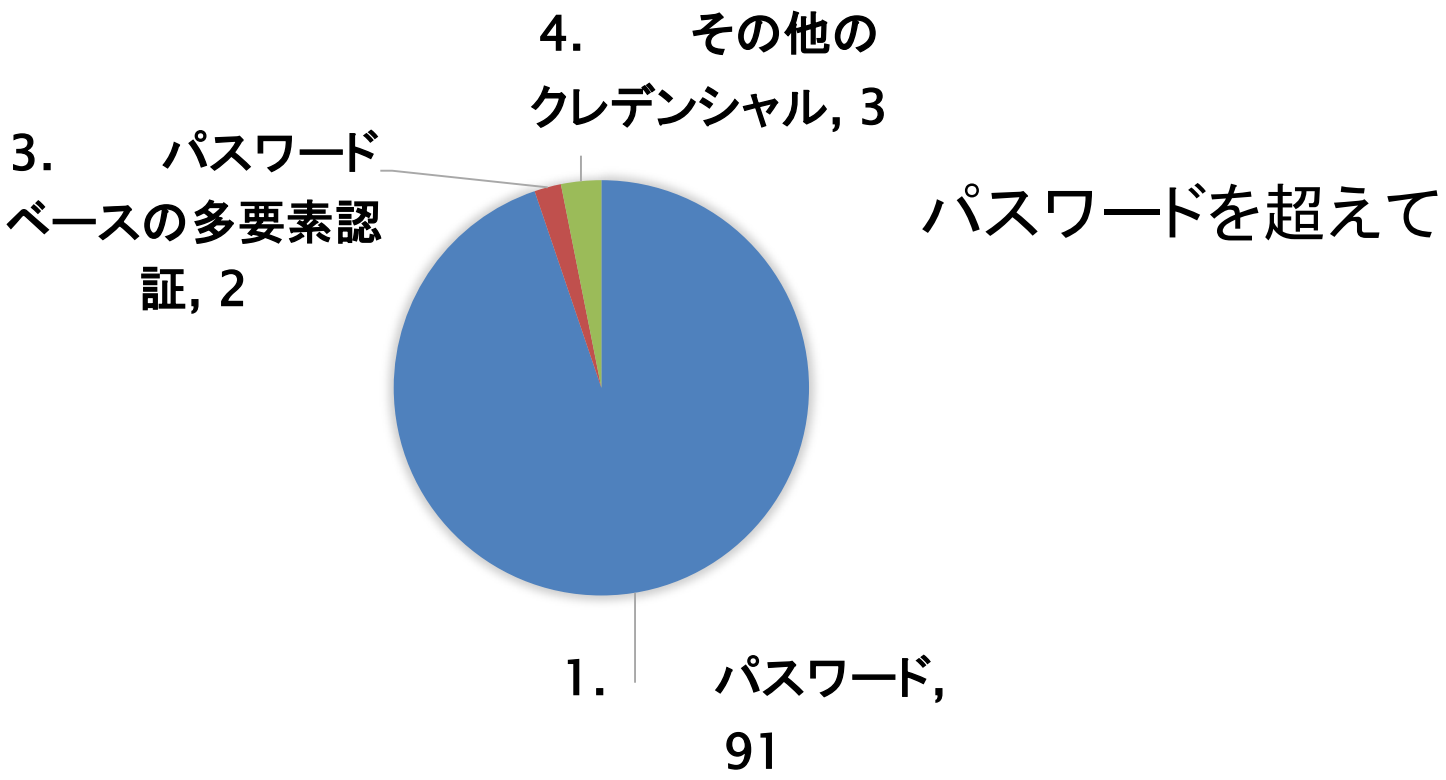
3. パスワードポリシーは定めておらず，特に啓蒙活動なども行っていない。，1



パスワードポリシー

1. パスワードポリシーを定めている。，150

パスワードを超えて



学認のトラストへの取り組み

- 学認はKantara Initiativeに加盟するとともに、トラスト作業部会がKantaraのトラストレベル1（＝米FICAMのLoA 1）を認定できるようになりました
  - 学認の内部にありながら、一定の独立性をもってレベル認定を行う

- 「トラスト」は、サービス運用において重要な概念になっていますが、トラストの運用は、アメリカ、ヨーロッパも含め成熟までにまだ時間がかかるようです
- 運用に関する信頼性（アイデンティティの保証、属性値の保証等）を外部の目から保証するためにLoAは役に立ちます

保証レベル認定の流れ

- Kantaraの保証レベル認定の評価基準はIAF-1400 Service Assessment Criteriaとして公表されています

- 学認アンケートにpositiveに答えることができれば、保証レベル認定プロセスの多くの部分をアンケートへの回答で代替することができます

- 学認参加機関に関しては、バリアが低くなっているはずです。国際的な大学間研究協力や、企業のサービス利用を考えているところは積極的にご利用ください

今年は

- 今年の学認アンケートでは、参加機関の大幅な増加にも関わらず、成熟した運用を行っている機関が多くありました。
- 学認へ参加して、経験を積むことで運用が成熟してきたのなら、学認にとって大きな喜びです
- もうひとつ、新たに参加してきた機関で、（外部による）統制がきちんと効いていると考えられるところがありました
  - 運用レベルの底上げを図るには非常に有効な手段です
- 外部からの客観評価を含む統制の強化、技術の変化進展（認証に対するリスク評価等）へのキャッチアップが課題になるでしょう

発表！　IdP of the Year 2015

2016.5.27　学術情報基盤オープンフォーラム2016

学術認証運営委員会

IdP of the Year

- 2012 / 2013は，学認アンケートの結果をもとに，もっとも模範となるIdP運用機関を表彰
  - 2012: 大阪大学
  - 2013: 山形大学
- 2014では，学認アンケートの結果のみならず，IdPに関して，最も顕著な活動が見られた機関を表彰
  - 2014: 金沢大学
- そして，2015

  学術認証運営委員会において審議した結果は・・・


GakuNin
IdP of the Year 2015
国立高等専門
学校機構

IdP of the Year 2015　国立高等専門学校機構

- 2014年度に全国の高専が学認に一斉に加盟（51校＋機構本部）
- 2015年度も安定

その中で

- 全国の高専全体のマネージメント
- 各高専のIdPの運用管理レベルを高く保つ努力
- 運用レベルの下支えを全国レベルで実現

- 上が良好に運用されていることが、学認アンケート等で証明された！