「正しい認証基盤構築ガイド」ご案内 @NIIオープンフォーラム

佐藤周行
トラスト作業部会

はじめに

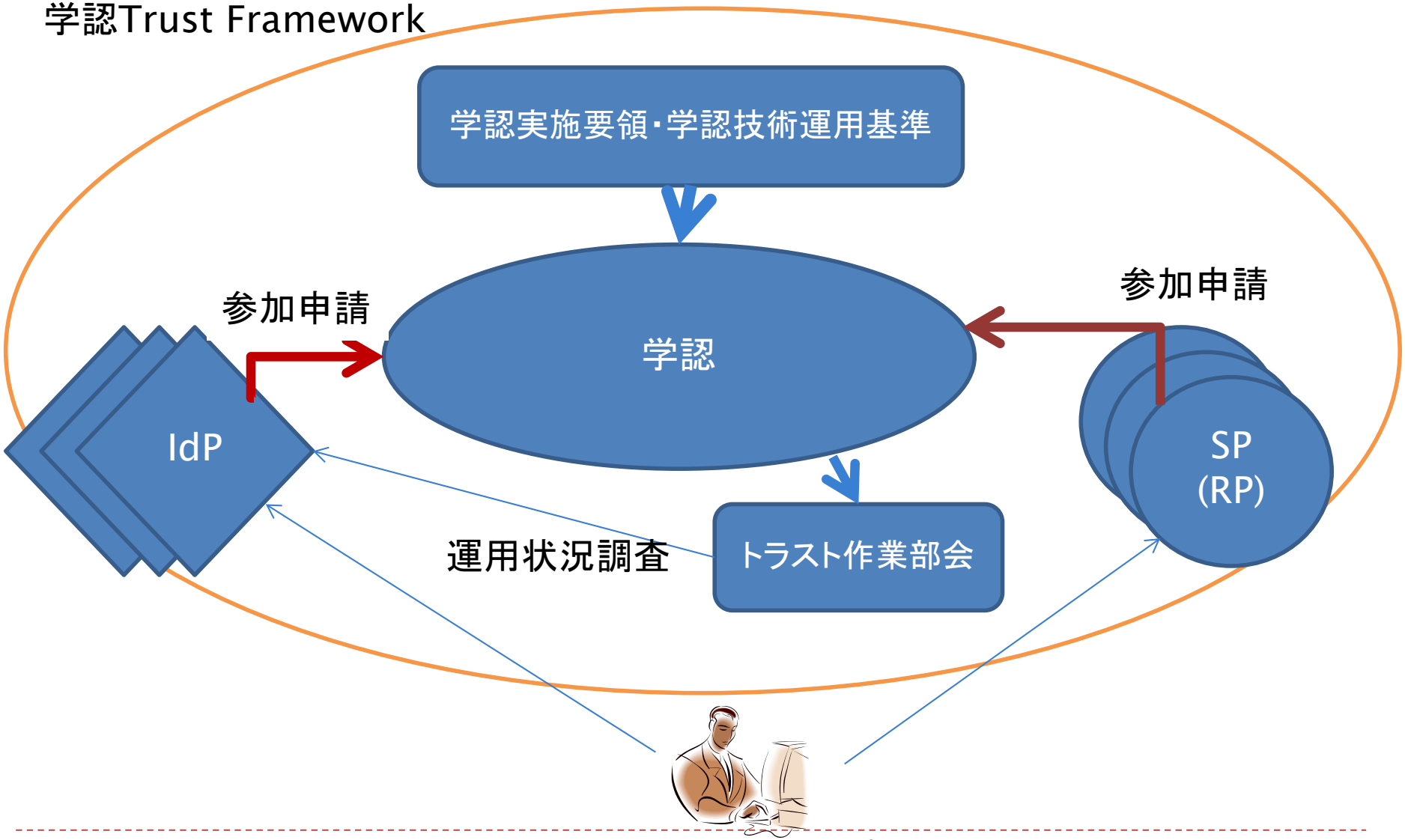
- 「学認」の立ち上がりからしばらく経ちました
  - 2008年～
    - 平成20年シングルサインオン実証実験（報告書あり）
  - 2014年よりNIIの事業に
  - 最初は「シングルサインオン」のためのプラットフォームであった
- Shibboleth based SSO Platform
  - Shibboleth since 2003.
  - USAでのInCommonnの立ち上げ
  - ヨーロッパでの国ごとのFederationの立ち上げ
- eduGain
  - Federation of Federations
    - 43 Full members, 5 voting members, 11 candidates (May, 2017)
    - Platform of Int'l Collaboration (LIGO etc.)

はじめに（続き）

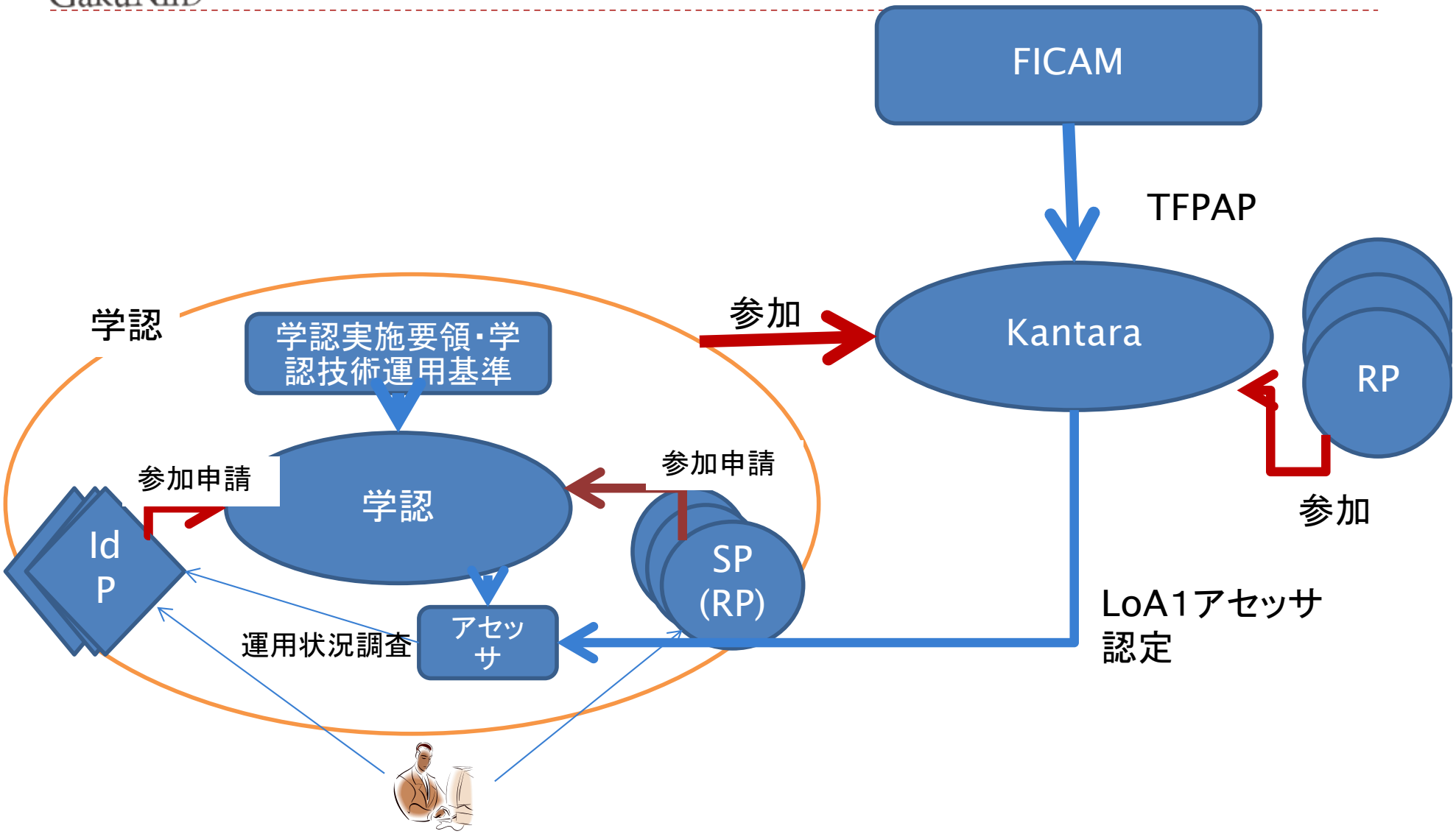
- Federation and Trust
  - Federation内でGovernanceのための規程整備が進んでいる
- 学認の場合は「学認実施要領」「学認技術運用基準」
  - IdPとSPの間の信頼の源泉
- これ（規程とそれに基づいた運用）を信頼してくれるところと新たなフェデレーションが組める
  - 学割
  - 国際研究協力

学認のトラストモデル

学認Trust Framework



国際標準への参加


FICAM
TFPAP
Kantara
参加
学認
学認実施要領・学認技術運用基準
学認
参加申請
参加申請
Id P
SP (RP)
RP
参加
運用状況調査
アセッサ
LoA1アセッサ認定

運用状況調査

- IdPの運用状況調査（旧学認アンケート）
- 自己申告制 & トラスト作業部会による精査
- 調査の目的
  - 学認参加IdPの運用が、規定通りになされているか
    - 学認実施要領
    - 学認技術運用基準
  - 自己申告に基づいた監査といった側面をもつ
- 対象機関
  - 2015年9月1日現在，学認の運用フェデレーションに参加しており，かつ IdP を設置している機関
- 調査方法
  - Excelの調査票配付による

精査時の 評価基準

1. 運用の統制（Control）．特に規則による統制
2. 運用アイデンティティの運用管理（アカウントのライフサイクル管理）
3. システムの構成管理（configの適切な管理）
4. パスワード（クレデンシャル）の管理

- これら基準にそって回答を個別に精査し、2段階で評価
  - A. 適切な運用のレベル
  - B. 改善の余地が認められるレベル

調査票の設計方針

- 設問は，学認を運営する学術認証運営委員会の下に組織されるトラスト作業部会が作成
  - 実施要領と運用基準への準拠性
  - LoA1認定の基準
- カテゴリごとに編成して調査票を構築
  - 一般的な項目について（いわゆるフェイス項目）
  - 利用者IDと属性の管理・運用について
  - 共有IDの禁止について
  - 個人情報保護について
  - 一般的なセキュリティについて
  - （任意）利用者IDおよびクレデンシャルについて
- 評価基準の検討
  - ガバナンス、テクニカル、プライバシー

IdP運用で注意すべき3要素

- ガバナンス
  - 運用の統制について．とくに運用規則が定められているか．
    - 「1．運用の統制（Control）．特に規則による統制」
- テクニカル
  - 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）
    - 「2．運用アイデンティティの運用管理（アカウントのライフサイクル管理）」
  - クレデンシャルの管理は適切か
    - 「4．パスワード（クレデンシャル）の管理」
  - 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
    - 「3．システムの構成管理（configの適切な管理）」
- プライバシー
  - IdPのデータは適切に扱われているか．とくに利用者の同意取得．
    - 「1．運用の統制（Control）．特に規則による統制」
    - 「3．システムの構成管理（configの適切な管理）」

「理想的なIdP運用」の例

- ガバナンス
  - 全学サービスセキュリティポリシーが定められている
    - その下にIdP運用規則，パスワードポリシー，プライバシーに関する規定がある
    - IdPはこれら規則のもとで適切に運用されている
- テクニカル
  - 利用者のIDおよび属性のデータベースはTrusted DBに基づいて作成されている
  - IDの再利用はない
  - 組織として保証する属性
    - O
    - eduPersonAffiliation
    - eduPersonEntitlement
    - eduPersonScopedAffiliation
    - eduPersonTargetedID
- プライバシー
  - IdPから送出される個人情報は，関連する法令その他に従うよう運用されている
  - 属性送信時の利用者同意取得のために，Shibboleth IdP Version3の属性リリース同意取得機能を使っている

LoA1認定に向けて

- KantaraのLoA1認定評価基準
  - Organizational Criteria（サービスとそれを提供する者のビジネス・組織の面からみた適合性）
    - 組織的な成熟はみられるか
    - サービスが正式なものとして組織から提供されているか
    - 組織は認証サービスを提供するときに不可欠なプライバシーについて法令を遵守し，さらに配慮を払っているか
  - Operational Criteria（クレデンシャル管理をはじめとする技術的，運用的な適合性）
    - クレデンシャルのライフサイクル管理は正しくされているか
    - 認証強度は十分か
- これら評価基準は，学認アンケートでの評価基準と親和性が高く，容易にマッピングすることができる
- Organizational CriteriaとOperational Criteriaの双方で基準を満たすことは難しくない
- 保証強度認定のプロセスの多くを学認アンケートへの回答で代替することができるので，学認参加機関におけるLoA1認定への障壁は低くなっています．
- 国際的な大学間研究協力や，LoA1認定を必要とするサービスの利用を考えている機関は，学認の認定制度を活用することができるので，検討していただきたい

IDaaSの活用

- IDaaS，つまり認証基盤を提供するクラウドサービスに，学認に対応したもの，対応を予定するものが散見されるようになった
- ガバナンス
  - 学認参加機関による規程の整備が主であり，IDaaSのカバーする範囲ではない
  - IDaaS側に，各機関のコンテクストに立脚した規程の差異を設定変更などで吸収できる，ある程度の柔軟性があればよい
- テクニカル
  - Trusted DBとの接続が問題
  - 直結してIDおよび属性情報の取得が行えることが望まれますが，一方でこれを許可する機関が多くないことも容易に想像できる
  - IDaaSが保持するデータベースが，Trusted DBに基づいて生成されるように手段を講じることになると思われる
    - 換言すれば，問題になるのは Trusted DB への接続のみ
  - IDの再利用はなされないように設定，属性については学認が推奨する属性を保証できるようにし，機関が利用したいSPが必要とするものを送出するよう設定できればよい
- プライバシー
  - IDaaSが果たせる役割が大
  - 法令に準拠した個人情報送出
  - 属性リリース同意取得機能は，Shibboleth IdPv3の機能を用いてもよいし，独自実装でも問題はない

調査の結果

- 2016年度については、後から報告があります

- おおむね良好な結果が得られています
- 2016年度は、すべての機関から回答が得られました

- 統計は2015年度のものを使っています。
- 詳細はWebで

「学認アンケートを通して学ぶ正しい認証基盤構築ガイド」

https://www.gakunin.jp/?action=repository_uri&item_id=248

また、以下で発表しています

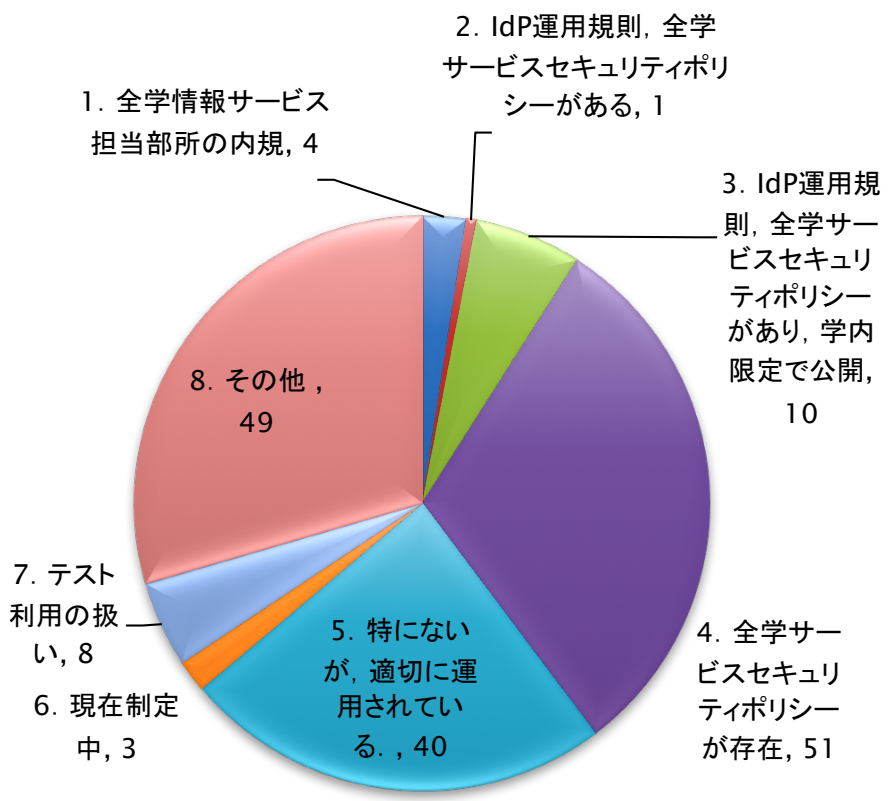
水元他：**日本のアカデミアにおけるアイデンティティ管理の現状 ―学認アンケートからみる現状の理解と将来の展望―，コンピュータセキュリティシンポジウム CSS 2016, 秋田**

ガバナンスについて０

- 総評において，IdP運用上の規程類整備の重要性を指摘
- IdP運用上の規則が制定されていない場合，IdPを運用する担当者の裁量が大きいと見なすことが出来る．
  - 詳しい者が適切に運用しているので問題ない，という考え方は，多様な問題を潜在させ，放置していることに他ならない．
  - 未整備の場合は「幸いにして」問題が顕在化していないうちに，早急に制定することが望ましい．
  - なお，より上位の規則を定めた上で，IdPの運用規則を整備することを推奨している
    - たとえば全学のセキュリティポリシーがあり，その下でIdP運用規則がある，といったケースがあげられる．
    - 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たので，参考とされたい．
- 規程類は，権限を適切に実施する統治力を備え，死蔵されることなく，継続してメンテナンスし，陳腐化を防ぐことが求められる

ガバナンスについて 1

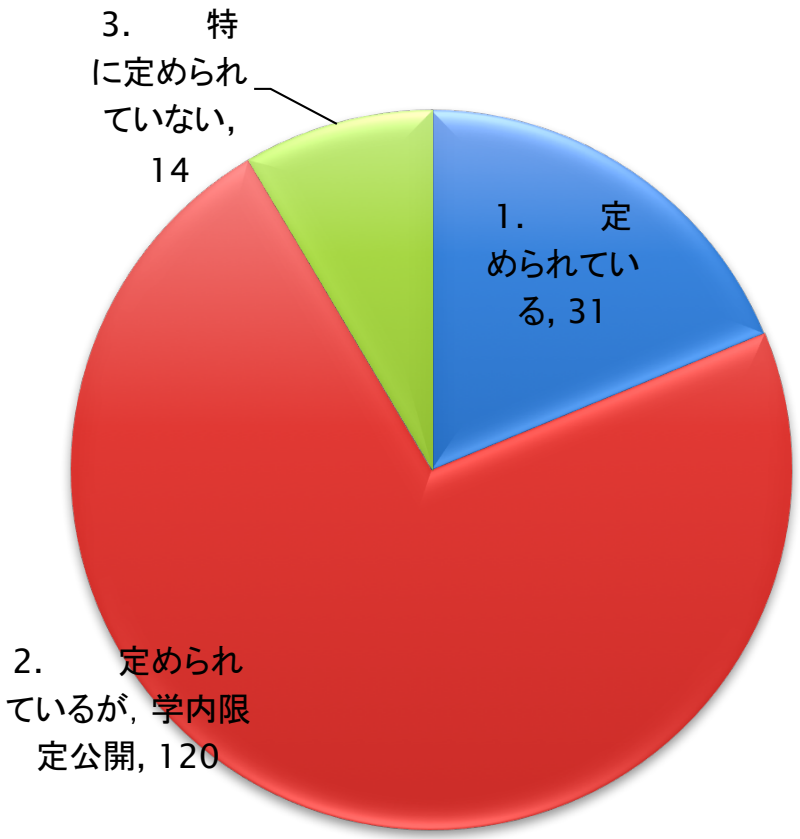
Q8 IdP運用上での根拠規則や内規の制定状況について



○	1. 全学情報サービスを担当する情報基盤センターの内規がある. 14
○	2. IdP運用規則, 全学サービスセキュリティポリシーがある. 1
○	3. IdP運用規則, 全学サービスセキュリティポリシーがあり, 学内限定で公開されている. 10
○	4. 全学サービスセキュリティポリシーが存在する. IdPはそのもとで適切に運用されている. 51
	5. 特にないが, 運用責任者の管理の下, 適切に運用されている. 40
	6. 規則などは特にないが, 現在制定中である. 3
	7. 全学的にはテスト利用の扱いになっている. 8
	8. その他 49

ガバナンスについて 2

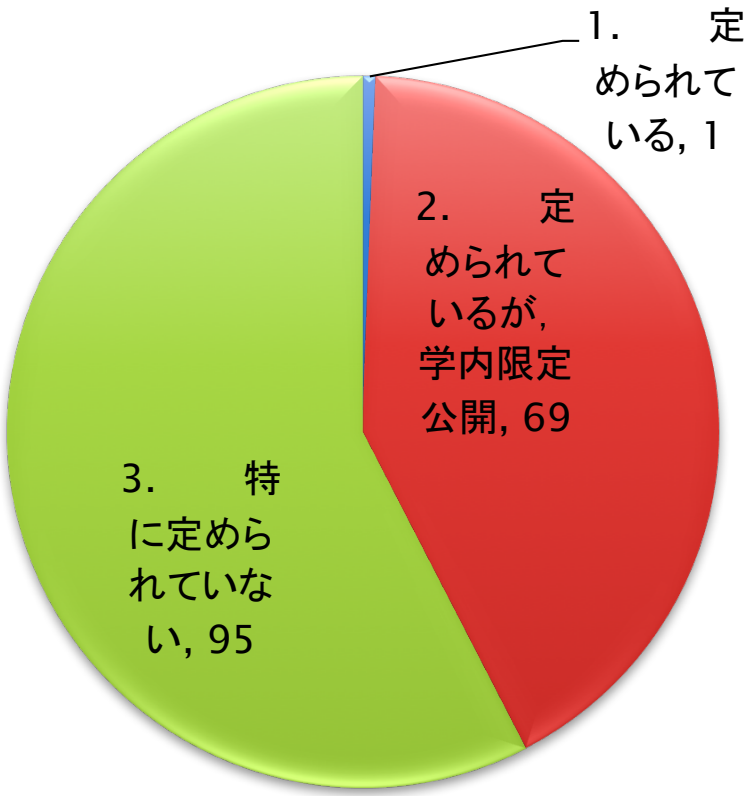
- Q29上位の全学または部局のセキュリティポリシーが定められ，それに従って運用されているか



○	1. 定められている．31
○	2. 定められているが，学内限定公開の扱いである．120
	3. 特に定められていない．14

ガバナンスについて 3

- Q30 IdP運用に関するセキュリティポリシーが定められているか



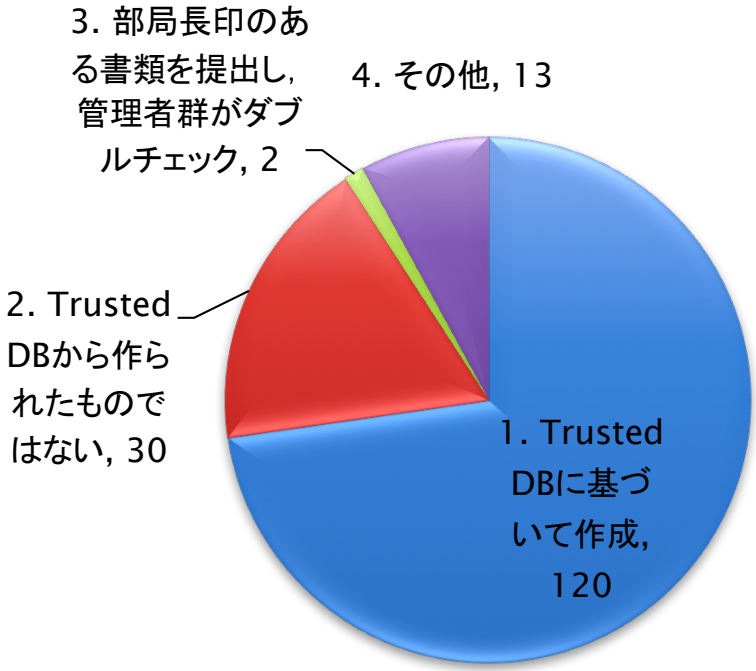
○	1. 定められている. 1
○	2. 定められているが, 学内限定公開の扱いである. 69
	3. 特に定められていない. 95

テクニカルなこと０

- IDの運用状況について
  - 利用者IDのソースとしては，Trusted DBと直接つながっているか，Trusted DBに基づいて生成されるものが望ましい
  - これら以外の手法では，今後のID数の増加，保持させる属性情報の増加に比例してその手間が増えていくという弱みを内包するものになる
  - スケーラビリティの観点から，ID管理をTrusted DBに直結する形で行えるよう，管理規則や事務フローの整備を勧奨する
- ゲスト・臨時アカウントについては，運用上作成せざるをえないケースがあることを承知しつつも，取り扱いには慎重さが要求されるものと考える
  - 発行は最小限として，記録を残し，また学認のサービスが利用できないようにするなど，権限の適切な制御を実施すべきである

テクニカルなこと 1

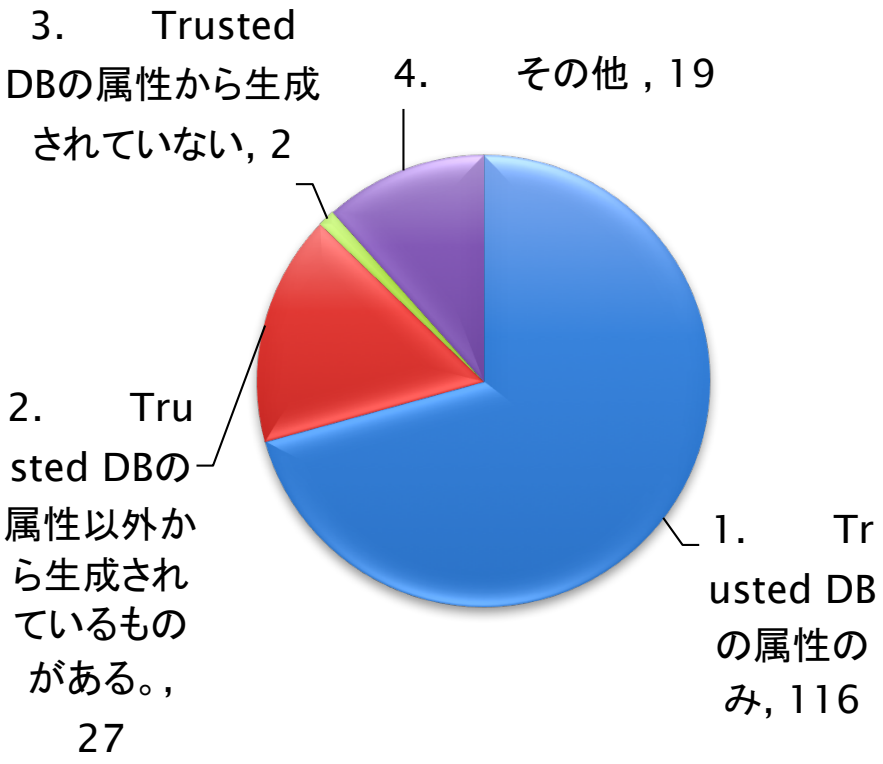
- Q9 IDの運用状況（Trusted DBと直結しているか）



○	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
	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から作られている．30
	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
	4. その他．13

テクニカルなこと 2

- Q15 IdPが送信する属性の信頼性は何によって保証されているか．たとえばTrusted DBから自動的に生成されるようになっているか



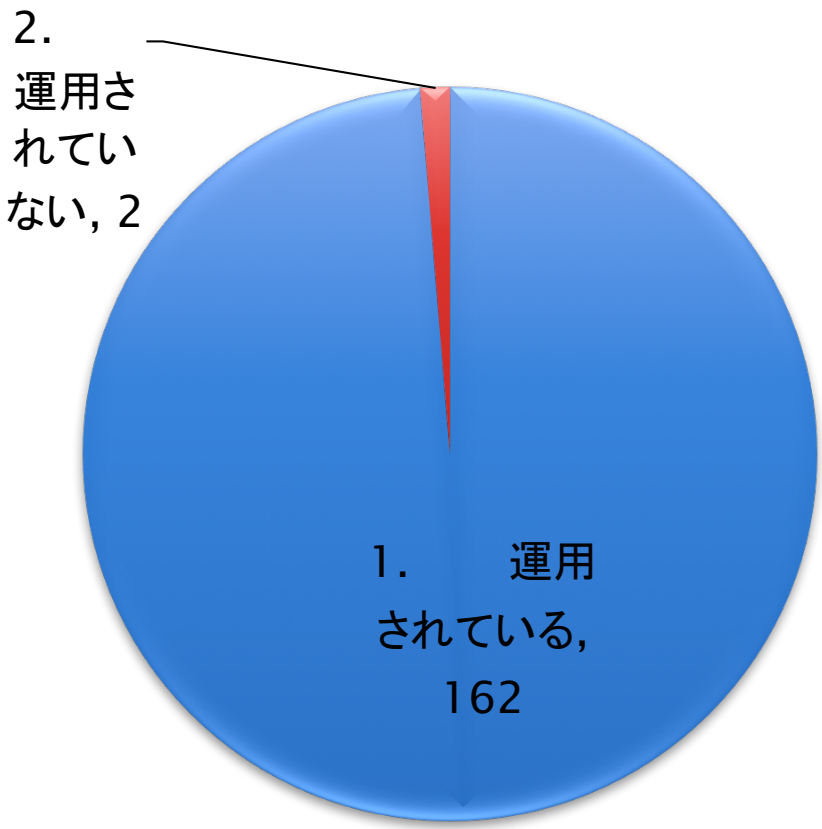
○	1. 利用者IDの属性は，Trusted DBの属性のみから計算されている．116
	2. 利用者IDの属性の一部には，Trusted DBの属性以外から生成されているものがある．27
	3. 利用者IDの属性は全て，Trusted DBの属性から生成されていない．2
	4. その他．19

プライバシーについて 0

- 「利用者合意」を得るのが基本形
  - IdP運用主体となる法的組織体の態様によって，個人情報保護法群のうちどれが適用されるかは異なるため，差異が生まれる
  - 数年前であれば「注意深く運用する」ことで対応できたものが，そうとは言えない現状にある．あるサービスを利用するにあたっての，同意を取得する手段を検討し，整備する段階にあると言える．
- 学認が推奨しているShibboleth
  - Version 2系統にはプラグインとしてuApprove
  - Version 3系統には組み込みの属性送信合意取得機能
    - これを用いて利用者合意を取得することができるので，是非利用すべきである．
  - Shibboleth v2系統はEOLが明示されており，使うべきではない

プライバシーについて 1

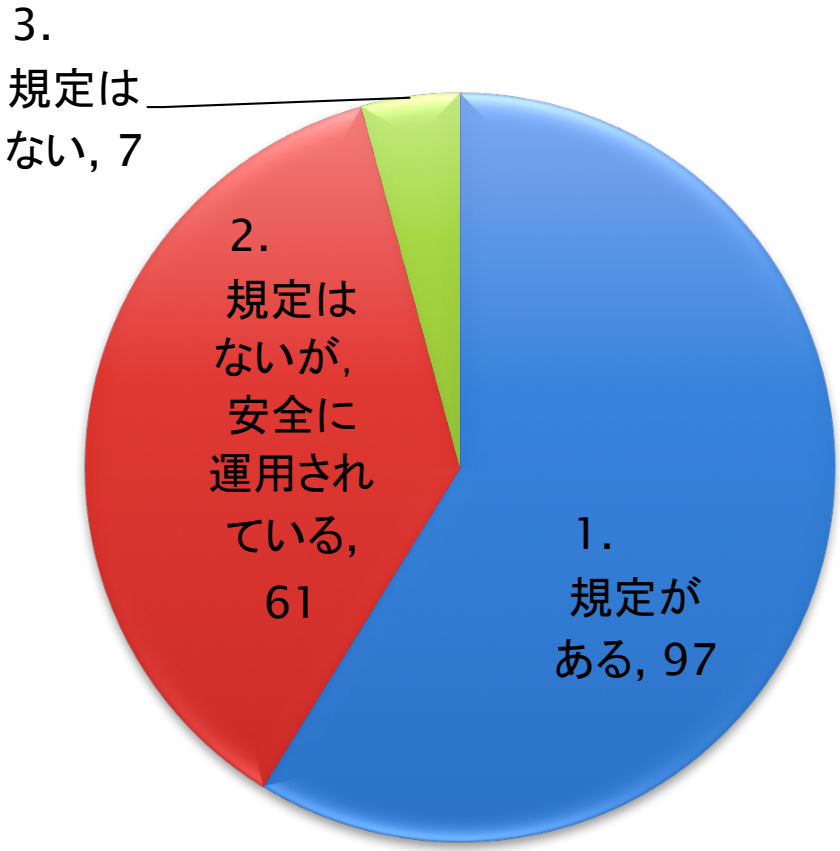
- Q24 IdPから送信される個人情報について，関係する法令その他に従うように運用されているか



○	1.　関連する法令その他に従うように運用されている.　162
	2.　関連する法令その他に従うようには運用されていない.　2

プライバシーについて 2

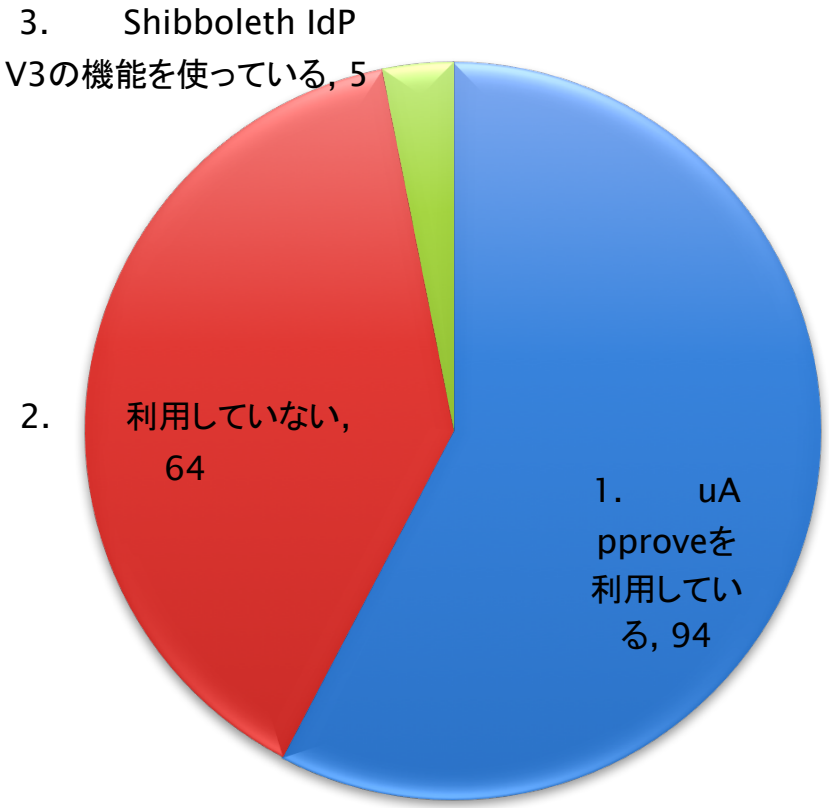
- プライバシーに関する規定の整備 Q25



○	1.　プライバシーについての具体的な規定がある．97
	2.　プライバシーについての具体的な規定はないが，利用者IDとその属性は安全に運用されている．61
	3.　プライバシーについての具体的な規定はない．7

プライバシーについて 3

- 属性リリースの同意取得



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

まとめにかえて

- IdPを適切に運用することにより、いろいろなご利益があります
  - トラスト
  - 他フェデレーションとの連携
- 「適切な運用」のためにどこに注力するかが大切です

- 「運用状況調査」の質問事項をチェックリストとしてご活用ください