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

学認トラスト作業部会

7 October 2016

1. はじめに

学認 IdP 運用機関の皆様には，毎年の学認アンケートへのご協力をいただき，まことにありがとうございます．学認アンケートは，全ての IdP 運用機関にご回答頂くことを必須としているものです．回答にはシステムと組織の双方への確認作業が必要なものが多く，担当頂く部所には多大なエフォートをさいていただいていることと思います．当然，学認参加後に初めて回答するときには，暗中模索する状況にあったことと思います．

毎年，回答頂いた機関にはフィードバックを行ってきましたが，それは回答に対する個別の修正点が主となっており，全体を俯瞰した改善点の指摘に至るものではありませんでした．設問にどのように回答するのがよいのか，その前段階として，システムと組織をどのように整備していけばよいのか．運営主体としての学認では，そういった道標をご提示していかねばならないということが，課題になっていました．

そこで学認トラスト作業部会では，本文書「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」を企画しました．

1.1 本稿の目的

本稿は，2015 年度に実施された「学認アンケート」の調査票[1]と総評[2]をもとに，学認アンケートにポジティブな回答ができるような IdP 運用とはどのようなものかを検討し，「理想的な IdP 運用」の一例を示すことを第一の目的としています．学認に参加する IdP 運用機関は，この「理想的な IdP 運用」と自機関の IdP 運用を，学認アンケートの回答をベースに比較検討することができるようになります．学認参加各機関による比較検討によって，学認全体の運用レベルの底上げに資することを第二の目的としています．

1.2 調査の概要

学認アンケートは，学認のポリシーとして定められている実施要領と，運用基準両者についての準拠性の調査として毎年実施しています．参加機関の自己申告に基づいた監査としての側面も持つものです．学認はトラストフレームワークであり，また実施要領と運用基準を定めるトラストフレームワークプロバイダでもあります．学認は運営主体として，学認参加機関による IdP 運用が規定通りになされているかをチェックする必要があり，学認アンケートは第一義としてこのために実施されます．

2015 年度の学認アンケートは，下記の通り実施しました．

1. 実施対象機関

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

2. 調査方法

Microsoft Excel で調査票を作成し，学認の Web サイトで公開しました．IdP 設置機関はそれをダウンロードして，メールで学認事務局に送付して回答しました．

3. 回答期間

2015 年 10 月 19 日から 11 月 20 日まで．

4. 回答数

167 機関からの回答をいただきました．

1.3 調査回答の評価

2015 年度学認アンケートの総評では，評価基準を以下の 4 点に定めています．

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

これらの基準にそって各機関からの回答を個別に精査し，「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」の 2 段階で評価しました．本稿で目指す「理想的な IdP 運用」が行われている機関は，この 2 段階評価では A を取得し，また個別の評価基準に関わる設問においても適切な回答ができることを企図するものです．

1.4 学認アンケートに適切に回答できることの付帯効果

学認アンケートには，回答した参加機関にも利点があります．先述の通り，学認はトラストフレームワークとして作用します．この枠組みで運用される IdP は，学認アンケートのような定期的な監査に適切に回答することによって，LoA: Level of Assurance (認証の保証強度)について一定の保証を受けることが出来ます. SP 側の視点から俯瞰すれば，自らが信頼性の基準を検討し，一つ一つ策定していくような手間を省くことができます．ネットワークを介するやりとりで必要な「信用」を作り上げるためのコストを下げることができ，そのリソースをサービスの向上にさくことができるようになります．学認アンケートの総評は先述

1 “学認アンケート調査票（平成 27 年実施版）”. http://id.nii.ac.jp/1149/00000235/, (参照 2016-07-14).

2 “学認アンケート総評（平成 27 年実施版）. ”http://id.nii.ac.jp/1149/00000236/, (参照 2016-07-14).

の通り公開されているので，SP は，学認がトラストフレームワークとしてどの程度作用しているのかを毎年知ることができます．

学認では，米国 ICAM: Identity, Credential, & Access Management[3] で定める 4 段階の認証の保証強度[4]のうち，LoA1 信頼性認定を行うプログラムを提供しています．LoA1 は世界標準と言える，IdP の認証の保証強度のベースラインです．こういった基準を定めることで，IdP はその基準を満たした信頼性のある ID 発行が行われていると主張することができ，また SP は LoA1 の保証強度を前提としたサービスの構築を行えるようになります．この保証強度の認定は TFPAP: Trust Framework Provider Adoption Process[5] に参加する認定機関によって行われるものです．学認は TFPAP のメンバーではありませんが，TFPAP の認定トラストフレームワークである Kantara に加盟するトラストフレームワークです．学認は Kantara に加盟[6]し，また Kantara における評価者資格を取得することで，参加機関に LoA1 の認定ができるようになっています．

LoA1 には，評価基準が設定されています．こうした基準を満たせているかを評価者が判断する際に，学認アンケートへの回答が大きな領域を占めます．学認アンケートにポジティブな回答がなされていると，LoA1 相当もしくはそれ以上の運用が出来ていると言えるよう，設計がおこなわれているからです．第 2 章では調査票設計の方針と評価基準の設定について述べ，学認アンケートの回答とその評価にふれます．

2. 学認アンケート調査票の設計方針と回答の評価

2.1 調査票の設計方針

学認アンケート調査票の設問は，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します．学認アンケートは先述の通り実施要領と運用基準への準拠性確認のために実施されるので，準拠性を確認しなければならない条項を洗い出し，そこへのポインタを示しつつ，個別の設問を作成しています．さらに LoA1 認定の基準をもとに設問を作成し，これらをカテゴリごとにまとめ，調査票を構築しています．2015 年度調査では，「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」の 6 カテゴリにわけました．そのうち最後の 1 つは任意回答となっています．設問は，前年との比較を行うため基本的に同内容となっていますが，前年の回答率や精度をふまえ，文面や回答の方式を変更するといったことが行われています．

設問が出そろった段階で，評価基準の検討もあわせて行っています．評価基準は年度毎に設定され，前年と異なる場合もあります．

学認アンケートへの回答は，IdP 運用で注意すべき 3 点，すなわちガバナンス・テクニカル・プライバシーにそって抽出・再配置され，先述の評価基準による総合評価とあわせて報告書としてまとめられます．報告書は，最新のものまで学認の Web サイトから取得可能です．

2.2 IdP 運用で注意すべき 3 要素と評価基準の対応

一般的に IdP 運用で注意すべきことは，ガバナンス，テクニカル，プライバシーの 3 点です．

(1) **ガバナンス**

1. 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．

2015 年度学認アンケートの評価基準では「1．運用の統制（Control）．特に規則による統制」に該当します．

(2) **テクニカル**

1. 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）

2015 年度学認アンケートの評価基準では「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）」に該当します．

2. クレデンシャルの管理は適切か

2015 年度学認アンケートの評価基準では「４．パスワード（クレデンシャル）の管理」に該当します．

また以下の 3 項目は，2015 年度学認アンケートの評価基準では「３．システムの構成管理（config の適切な管理）」に該当します．

1. リモートの認証の手法は適切か

2. プロトコルは適切か

3. その他，一般的なシステムのセキュリティ

(3) **プライバシー**

1. 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．

2015 年度学認アンケートの評価基準では，「1．運用の統制（Control）．特に規則による統制」および「３．システムの構成管理（config の適切な管理）」に該当します．

次節以降，これら 3 点それぞれについて 2015 年「学認アンケート回答の精査報告」をもとに解説し，学認アンケー

3 “Federal Identity, Credential, & Access Management”. https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG,(参照 2016-07-14).

4 “NIST Special Publication 800-63-2”.http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf,(参照 2016-07-14).

5 “Trust Framework Solutions”. https://gsageo.force.com/IDM/s/article_content_old?tag=a0Gt0000000Sfwd,(参照 2016-07-14).

6 “Members –Kantara Initiative”. https://kantarainitiative.org/members/,(参照 2016-07-14)

トの設問への回答例をあげます．

2.3 ガバナンス

総評において，IdP 運用上の規程類整備の重要性が指摘されています．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ます．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りません．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と言えます．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ます．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ます．セキュリティポリシーに関する「サンプル規定集[7]」のうち，新たに定められた IdP に関する部分を参考にしてください．

また規程類は，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ものです．

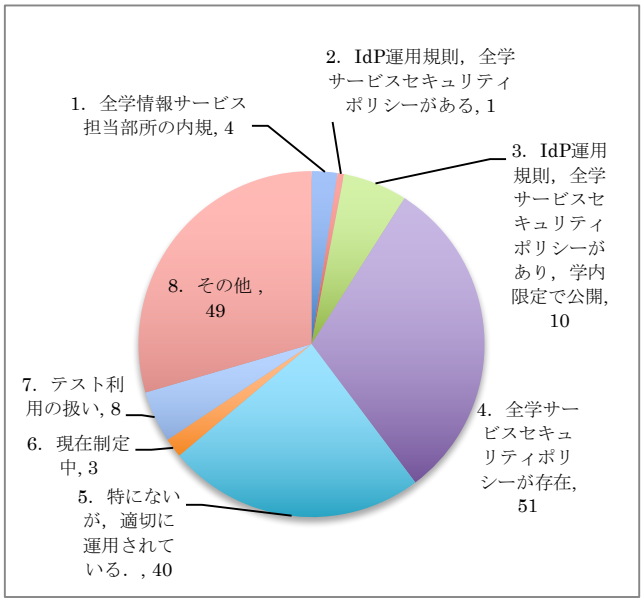
2.3.1 ガバナンスに関する設問の回答例

Q8: IdP 運用上での根拠規則や内規の制定状況について

IdP を運用する上での根拠規則や内規が定められていると回答した機関が，166 機関中 66 機関，約 40%ありました（図 1）．「その他」との回答が多くみられましたが，これらの回答の補足としてもうけられた自由記述欄をみると，規程の整備状況をより丁寧に説明したものが多くみられました．前年度調査では IdP の運用規則やポリシーの策定率が低く，半数を切っていましたが，今回の調査では半数以上の機関で整備されていると読み取ることができます．

回答としては，先述の通り，より上位の規則があり，さらに IdP の運用規則が定められていることが望ましいです．ですがいずれか片方でも，現時点での IdP 運用機関全体での整備状況を鑑みるに，可としてよいと考えます．回答としては，上位規則と IdP 運用規則をそろえる 2 と 3 が最もよく，次いで 4 と 1 を可とします．ただし 4 と 1 については今後の整備拡充を強く勧めます．外部に公開されている必要はありません．

図 1　Q8



○	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

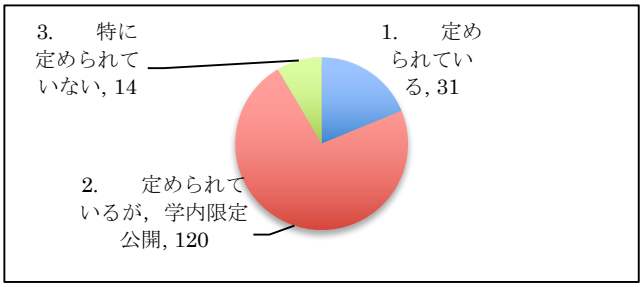
Q29: 上位の全学または部局のセキュリティポリシーが定められ，それに従って運用されているか

Q8 は IdP に限った設問ですが，Q29 はその上位に位置するセキュリティポリシーについての設問です．全学のセキュリティポリシーについては，151 機関，90%以上の大学で制定済みでした．また，定められていないとの回答が 14 機関ありました（図 2）．

全学あるいは部局のセキュリティポリシーが公開されているか否かに関わらず，定められていることが望ましく，よって回答としては 1 と 2 がよいでしょう．

7 “高等教育機関の情報セキュリティ対策のためのサンプル規定集（2015 年版補訂）”. http://www.nii.ac.jp/csi/sp/doc/sp-sample-2015s.pdf,(参照 2016-07-14).

図 2　Q29



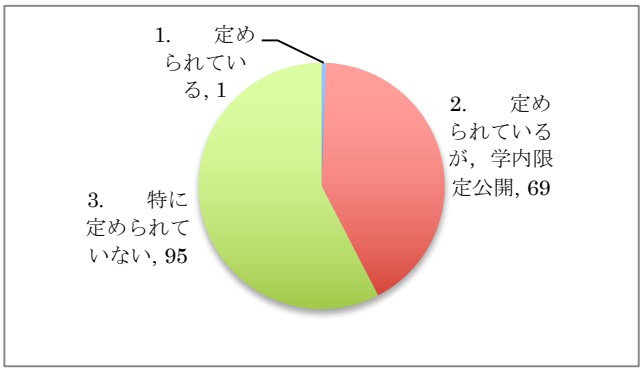
○	1.　定められている．　31
○	2.　定められているが，学内限定公開の扱いである．　120
	3.　特に定められていない．　14

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

Q30 は，とくに IdP が送出する属性の信頼性や正確性について定められものがありますか，という設問です．IdP 運用に関するセキュリティポリシーについては，70 機関，42%が定められていると回答しています（図 3）．

Q29 と同様，IdP 運用に関するセキュリティポリシーが公開されているか否かにかかわらず，定められていることが望ましく，よって回答としては 1 と 2 がよいでしょう．

図 3　Q30



○	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

2.4　テクニカル

ID の運用状況についてです．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です．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ってしまいます．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します．

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ます．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す．

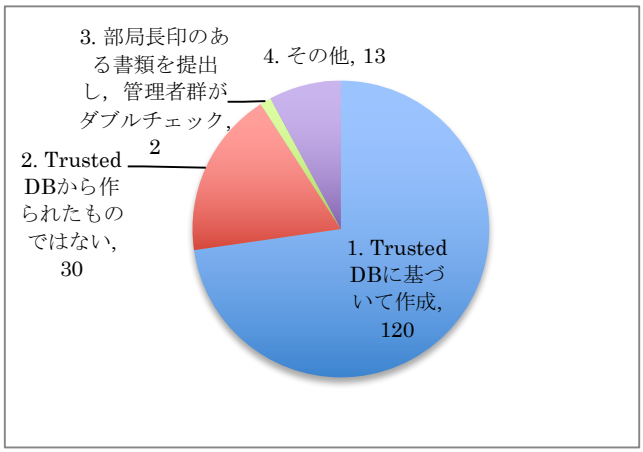
2.4.1 ID の運用状況（Trusted DB と直結しているか）に関する設問の回答例

Q9: 利用者 ID は，学務データや人事データ等，Trusted DB（組織にとって信頼できるデータベース）から作成されるように定めているか

利用者の ID は，120 機関において組織にとって信頼できるデータベース（ Trusted DB ）に基づいて作成され，また 30 機関において部局が責任を持って運用する DB をもとにしており（図 4），多くの機関で適切なユーザ管理がなされていると言えます．

ですが Trusted DB からアカウントを生成しなければ，今後のアカウント数の増加，管理属性の複雑化を見据えたスケーラビリティを確保できず，早晩行き詰まることが予想されます．よって回答としては 1 がよいでしょう．

図 4　Q9



○	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

2.4.2 属性保証に関する設問の回答例

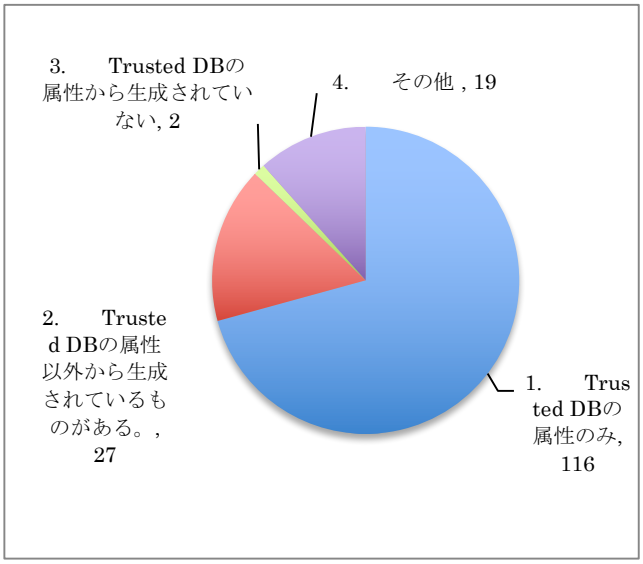
Q15: IdP が送信する属性の信頼性は何によって保証されているか．たとえば Trusted DB から自動的に生成されるよ

うになっているか.

属性情報については，116 機関において Trusted DB の属性のみから計算されているとの回答があり，また 27 機関において一部の属性は Trusted DB 以外から生成されているとの回答がありました（図 5）.

Q9 で述べた ID と同様，Trusted DB から属性も計算されるべきです．よって回答としては 1 がよいでしょう．2 は不可ではありませんが，別の問題として，複数のデータベースからの属性の生成には整合性の確認等，管理の手間が増すことが予想されます．よって学認では勧めません.

図 5　Q15



○	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

Q15b: 属性について，組織が保証しているものについて具体的にお答えください

ここでは，学認が利用を推奨する属性を列挙し，3 つにわけて重み付けを試みました.

組織が保証するべき属性

o と eduPersonAffiliation の両属性は，80%以上の機関で組織として保証されています．一方，「保証していない」と「未選択」をあわせて 20 程度の機関で保証されていないと読み取ることができます（図 6 と図 7）.

システムの設定，とくに学認の技術ガイドに基づいて Shibboleth が正しくセットアップされていれば，属性値 O は組織が保証できるはずです．特別な例として，複数の機関によって共同運用される IdP がありますが，こちらは単一機関が運用する IdP よりもとくに厳重に管理することで，自組織に所属しない者の属性を保証することができます．加えて，SP への不正な，利用資格を持たない者によるアクセスができないように，厳密な運用を行う必要があります.

また，アカウントが Trusted DB と直結して生成されているなら，属性値 eduPersonAffiliation も組織が保証できるはずです．この 2 属性の値は，組織が保証できるよう設定すべきであり，「組織が保証するべき属性」とします.

1.　o
2.　eduPersonAffiliation

図 6　属性 O

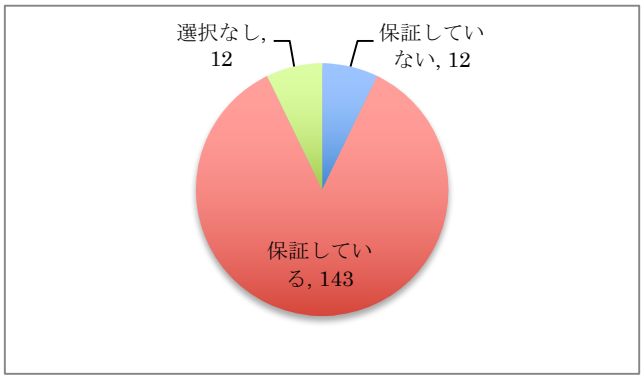
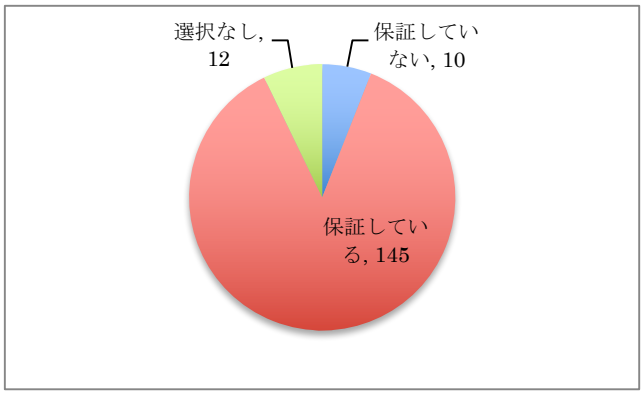


図 7　属性 eduPersonAffiliation



強く推奨する属性

多くの SP で利用されている以下の 4 属性も，組織が保証できるよう「強く推奨」します．ただし，これら 4 属性全てが送出できる必要はありません．とくにプライバシー保護のため，eduPersonPrincipalName は送出しないと定めている機関があります．機関のポリシーとの整合性と，利用したい SP が定める必須属性を考慮し，送信の要否を定めるとよいでしょう.

1.　eduPersonPrincipalName
2.　eduPersonEntitlement
3.　eduPersonScopedAffiliation
4.　eduPersonTargetedID

推奨する属性

1.　mail
2.　sn

3. ou
4. givenName
5. displayName
6. isMemberOf
7. jasn
8. jaGivenName
9. jaDisplayName
10. jao
11. jaou
12. gakuninScopedPersonalUniqueCode

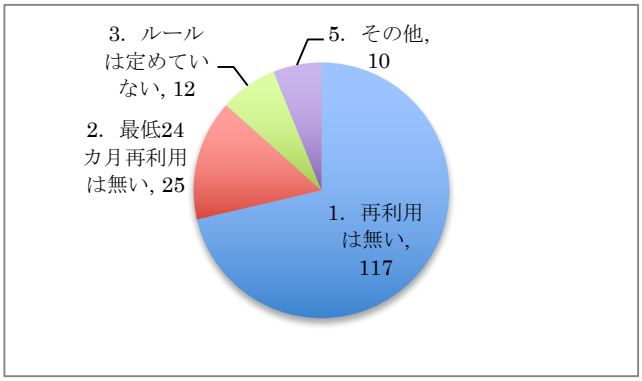
2.4.3 ID 再利用とクレデンシャルに関する設問の回答例

Q18: ID の再利用

ID の再利用については，142 機関で再利用はない，および最低 24 ヶ月間再利用はない，との回答でした．多くの機関において，適切な運用が確立されていると言えます（図 8）．

eduPersonPrincipalName ， eduPersonTargetedID を再利用する場合は，最終の利用時から最低 24 ヶ月あけることと学認技術運用基準で定めています．よってこれに準拠するため，回答としては 1 または 2 がよいでしょう．

図 8　Q18

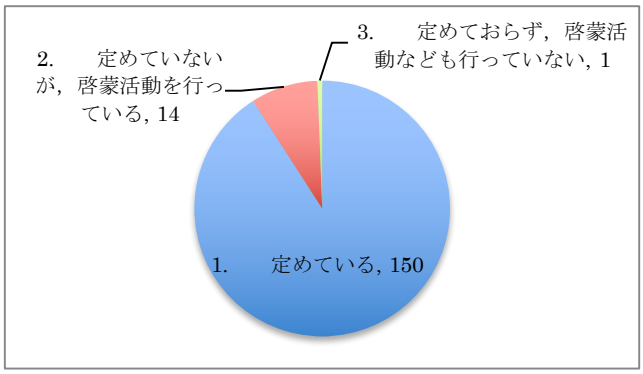


○	1. 再利用は無い 117
○	2. 最低 24 カ月再利用は無い 25
	3. ルールは定めていない 12
	4. 両属性の送出が必要となるサービスは利用していない 0
	5. その他．10

Q21: パスワードポリシーの制定状況

クレデンシャルの中でも，現在もなお主流となっているパスワードの管理については，パスワードポリシーによる管理，パスワードに対する攻撃の周知，パスワードが破られた場合の被害の理解で啓蒙活動を行うしかありません．今回の学認アンケートの回答ではおよそ 9 割の機関が「パスワードポリシーを定めている」と回答しており（図 9），整備が進んでいる状況にあります．必要性と各機関での整備の現状を鑑みると，回答としては 1 がよいでしょう．

図 9　Q21



○	1. パスワードポリシーを定めている． 150
	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

2.4.4 ログ保存期間に関する設問の回答例

Q28:ログの保存期間は定められていますか？　技術運用基準では推奨項目になっています.

本設問は自由記述としています．技術運用基準 8.7 では 3 ヶ月以上を推奨しているので，同等もしくはそれ以上の期間保存すると定めるとよいでしょう．

2.5 プライバシー

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が異なるので，若干の差異が生じますが，「利用者同意」を得るのが基本形といえます．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，今日はそうとは言えない現状にあります．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ます．学認が推奨している Shibboleth IdP であれば，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同意取得機能が提供されており，いずれかを利用することで利用者同意を取得することができるので，是非利用すべきです．

ただし Shibboleth IdP v2 系統はすでに EOL をむかえており，使い続けるべきでないことは言うまでもありません．

2.5.1 プライバシーに関する設問の回答例

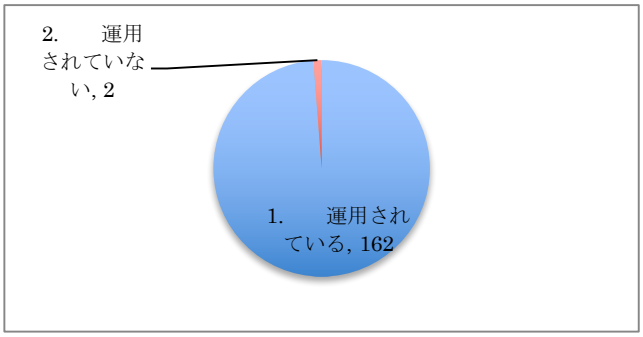
Q24: IdP から送信される個人情報について，関係する法令その他に従うように運用されているか

IdP から送信される個人情報について，162 機関，99%が関連する法令に従うように運用されていると答えました（図 10）．

学認実施要領第 12 条一号において，「IdP が提供する個人情報の取扱いに関し，法令の定めによるほか，委員会が別に定める規程等を遵守すること.」と定めています．IdP

運用機関は実施要領の内容を遵守するとして参加申請をしているので，本設問への望ましい回答は 1 となります．

図 10　Q24



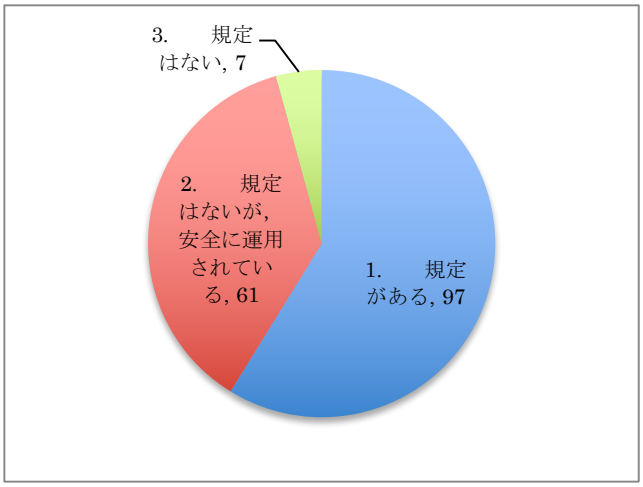
○	1.　関連する法令その他に従うように運用されている．　162
	2.　関連する法令その他に従うようには運用されていない．　2

Q25: プライバシーに関する具体的な規程はあるか

97 機関，57%がプライバシーについての具体的な規程があると回答しています（図 11）．

本稿では，規程類の整備による統治について述べてきました．プライバシーについての具体的な規程を定めて運用することは，法的組織体の責任であり必須と言えます．回答としては 1 がよいでしょう．

図 11　Q25



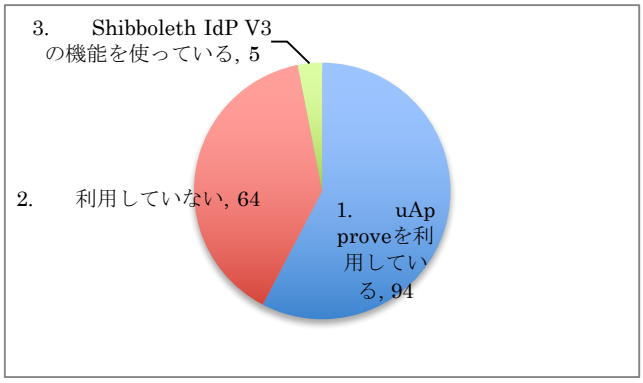
○	1.　プライバシーについての具体的な規定がある．　97
	2.　プライバシーについての具体的な規定はないが，利用者 ID とその属性は安全に運用されている．　61
	3.　プライバシーについての具体的な規定はない．　7

Q26: 新たな SP のサービスを利用するとき，属性リリースの同意を得るために uApprove もしくはその派生版を利用しているか

99 機関，59%が属性リリース同意取得機能を利用していると回答しています（図 12）．前年度調査では 70 機関 51%が同機能を利用しており，機関数，また割合としても前年より上昇しています．

プライバシー保護に関する法令の整備と改訂がすすみ，現状，IdP からの属性送出は，uApprove のようなシステム化された同意取得によるオプトインの方式に基づいて行われるべきです．よって，回答としては 1 または 3 がよいでしょう．

図 12　Q26



○	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

3.　学認アンケートをもとに構築した IdP 運用のモデル例

3.1　「理想的な IdP 運用」の例

ここまでの記述をもとに，「理想的な IdP 運用」の例を，IdP 運用で注意すべきガバナンス，テクニカル，プライバシーの 3 点にそって述べます．

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，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ります．IdP はこれら規則のもとで適切に運用されています．

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ます．ID の再利用はありません．組織として保証する属性は下記の通りとなっています．

1.　O
2.　eduPersonAffiliation
3.　eduPersonEntitlement
4.　eduPersonScopedAffiliation
5.　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ます.

また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ます

3.2 LoA1 認定に向けて

Kantara では，LoA1 認定のための評価基準を以下のように設定しています[8].

- 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

これらの評価基準は，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ものです. 本章で述べてきたような理想的な運用が行われていれば，Organizational Criteria と Operational Criteria の双方で基準を満たすことは難しくはありません．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，検討してください.

3.3 IDaaS の活用と導入時のヒント

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りました．本節では，3.1 で述べた「理想的な IdP 運用」の例をもとに，IDaaS の利用についての考察を行います.

まずガバナンスについては，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ありません. 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でしょう.

テクニカルな面では，Trusted DB との接続が問題になるでしょう．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ます．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でしょう．換言すれば，問題になるのは Trusted DB への接続のみです. ID の再利用はなされないように設定されればよいですし，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でしょう.

プライバシーについては，IDaaS が果たせる役割が大きいでしょう．そもそも法令に反した個人情報送出を行う製品は販売されませんし，属性リリース同意取得機能は，システム化して組み込みがしやすいものです．Shibboleth IdPv3 の機能を用いてもよいですし，独自実装でも問題はありません.

IDaaS の導入は，認証基盤を丸ごと外部に任せるような状態になります．ですが機関の監督から離れてしまうことは，当該機関と IDaaS 双方にとってよいことではありません．本節で述べたように，最低限，規程の管理にかかわる部分を押さえておく必要があります．十分に機能する規程であれば，IDaaS の運用も適切な方向に導くことができます．まだ事例としては少なく，ここで述べた「十分に機能する規程」の具体的な書き方については今後の課題となりますが，IDaaS 導入時に検討課題としてあげておくとよいでしょう.

4. おわりに

本稿で述べた「理想的な IdP 運用」の体制は，ただちに導入できるような簡単なものではありません．その多くの要素は組織的な整備を要するもので，また IdP 運用の各機関の内情にあわせてカスタマイズする必要もあるでしょう. しかしながら 1 つの道標として理想的な IdP 運用の態様を提示することは，それ自身と，ある IdP 運用機関との差異を浮き彫りにする効果が期待できます.

2015 年度の学認アンケートで 「A. 適切な運用のレベル」と評された機関は，さらなる高水準の運用を目指していってください．また「B.改善の余地が認められるレベル」と評価された機関は，フィードバック（すでに IdP 運用機関の運用責任者宛に送付済です）を理解したうえで運用の改善を行ってくださるようお願いして，本文書の結びとします.

8 “Kantara IAF-1400 Service Assessment Criteria v4.0bis”. http://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework ,(参照 2016-07-14)