2018年度学認参加IdP運用状況調査 総評

学術認証運営委員会トラスト作業部会

1 評価結果

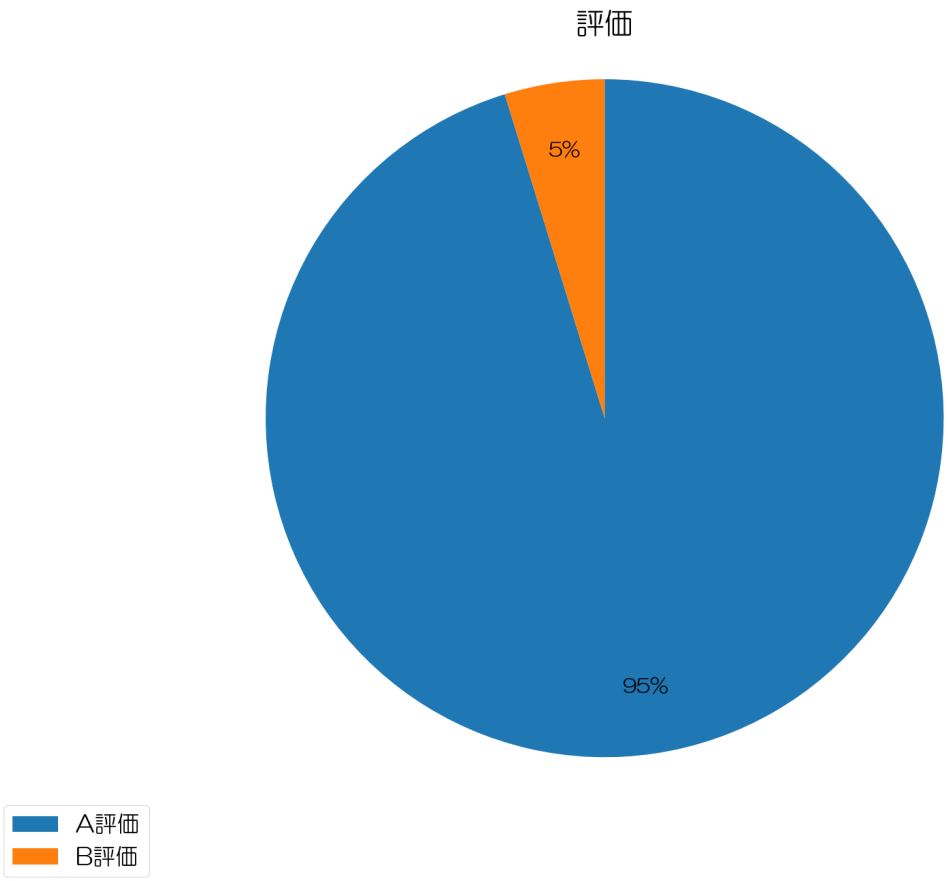
調査への回答機関数は210件です。適切な運用を行っている機関が200件となり、全体として良好な運用レベルです。一方、安定した運用のためには規程類の整備等が必要とみられる機関が10件みられました。

本調査の評価は、前年度同様、下記の基準で実施しました。

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
5. 設定ファイルの管理体制について
6. Shibboleth IdPの運用に関わるミドルウェア群のアップデート状況
7. Shibboleth IdP version 2系統がEOLを迎えたことによる、version3系統へのアップグレード状況

この基準に従って、組織全体としてIdP運用のレベルが保たれているか、すべての機関の回答を個別に精査しました。学認参加機関全体として、おおむね良好なIdP運用が行われていると判断することができます。

総じて前年度調査に続き、高い水準でIdPが運用されていたことが読み取れました。回答の傾向も、昨年からかけ離れたものはありませんでした。また、前年度B評価だった機関のうち、6件が今回の調査でA評価を取得しています。学認参加の各機関には、引き続きの運用をお願いいたします。



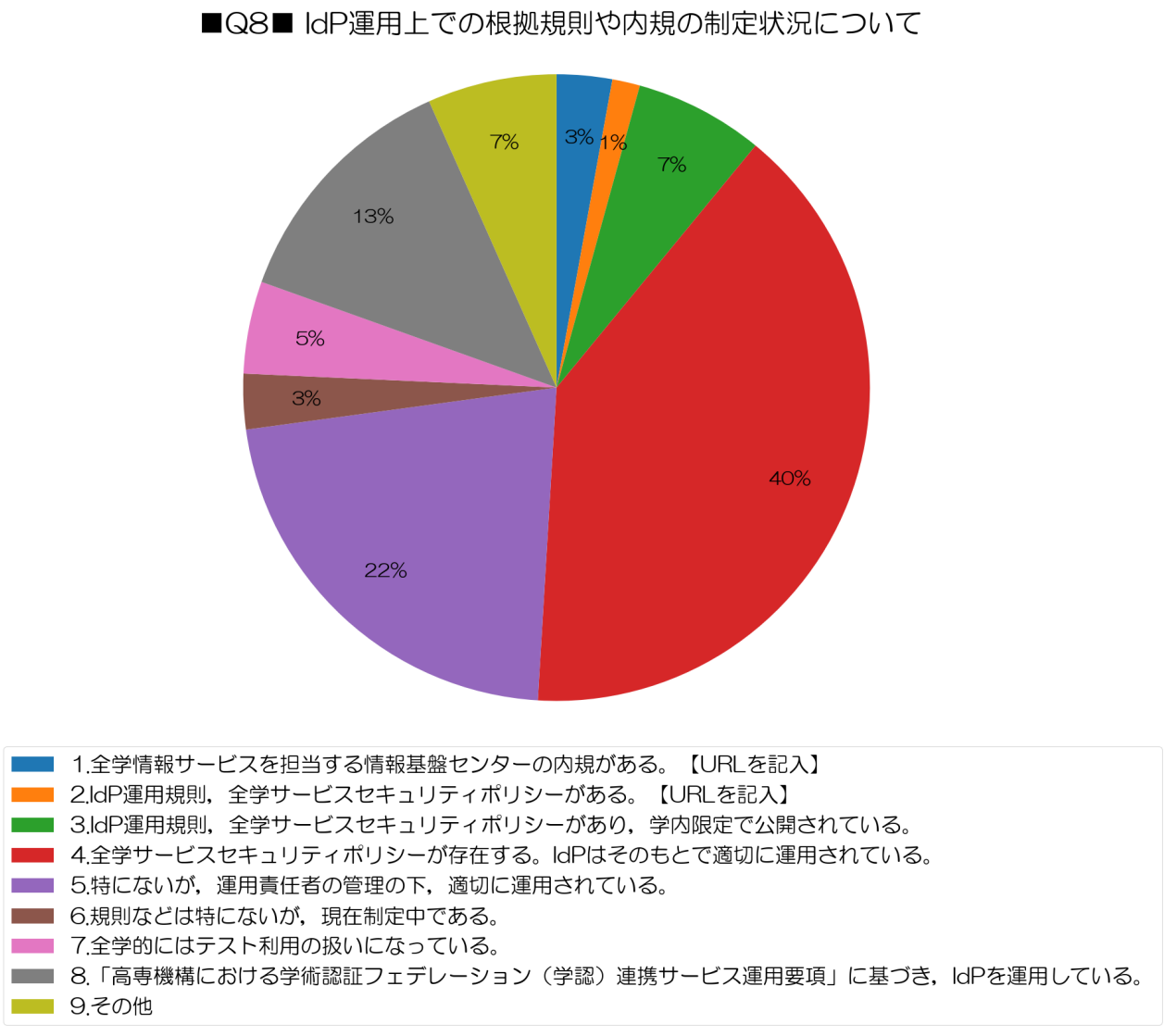
	機関数
A評価	200
B評価	10

2 ガバナンス（規程の作成状況）

全学のセキュリティポリシーについては、194件と90%近くの大学で制定済みですが、定められていないとの回答が16件ありました(Q30)。なお、IdP運用に関するセキュリティポリシーついては79件（38%）が定められているとの回答でした(Q31)。

多くの機関において、利用者IDの管理体制や全学的なセキュリティポリシーが整備されています。その基盤の上になりたってIdPが適切に運用されていることが読み取れます。Q8において、なんらかの規程が整備されているとの回答は134件ですが、その他 14件の自由記述の内容を読んでいくと、規程の整備状況をより丁寧に説明したものが多く見られました。前年度調査の結果に続き、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。

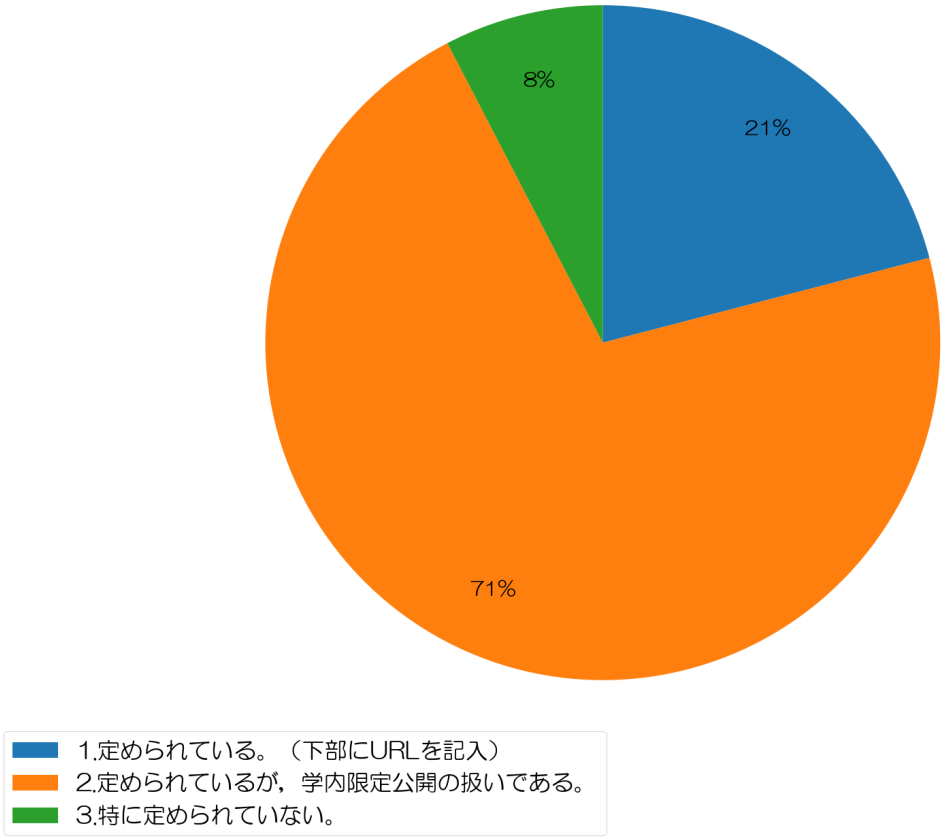
Q-8



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。【 URLを記入 】	6
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。【 URLを記入 】	3
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。	14
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。	84
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。	46
6. 規則などは特にないが，現在制定中である。	6
7. 全学的にはテスト利用の扱いになっている。	10
8. 「高専機構における学術認証フェデレーション（学認）連携サービス運用要項」に基づき，IdPを運用している。	27
9. その他	14

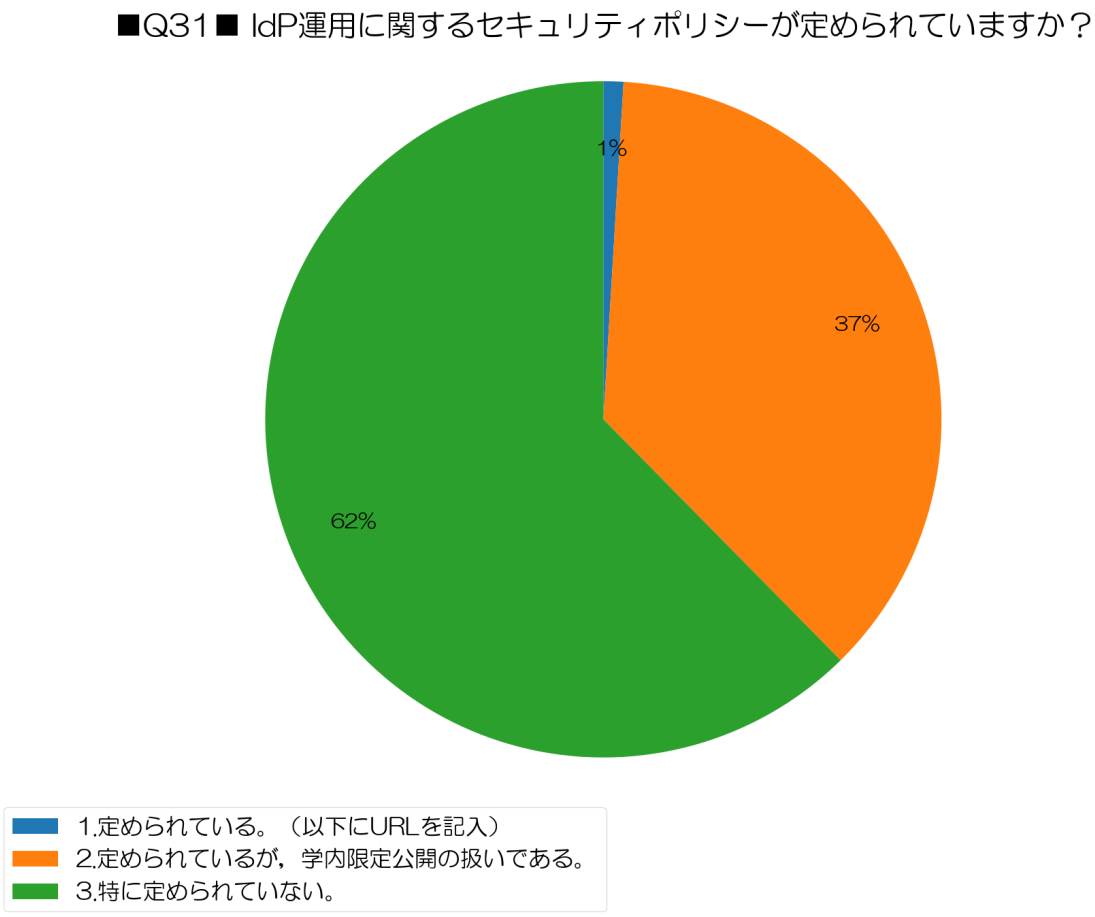
Q-30

■Q30■ 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，
それにしたがって運用されていますか？



1. 定められている。（下部にURLを記入）	44
2. 定められているが，学内限定公開の扱いである。	150
3. 特に定められていない。	16

Q-31



1. 定められている。（以下にURLを記入）	2
2. 定められているが，学内限定公開の扱いである。	77
3. 特に定められていない。	131

3 テクニカルなこと

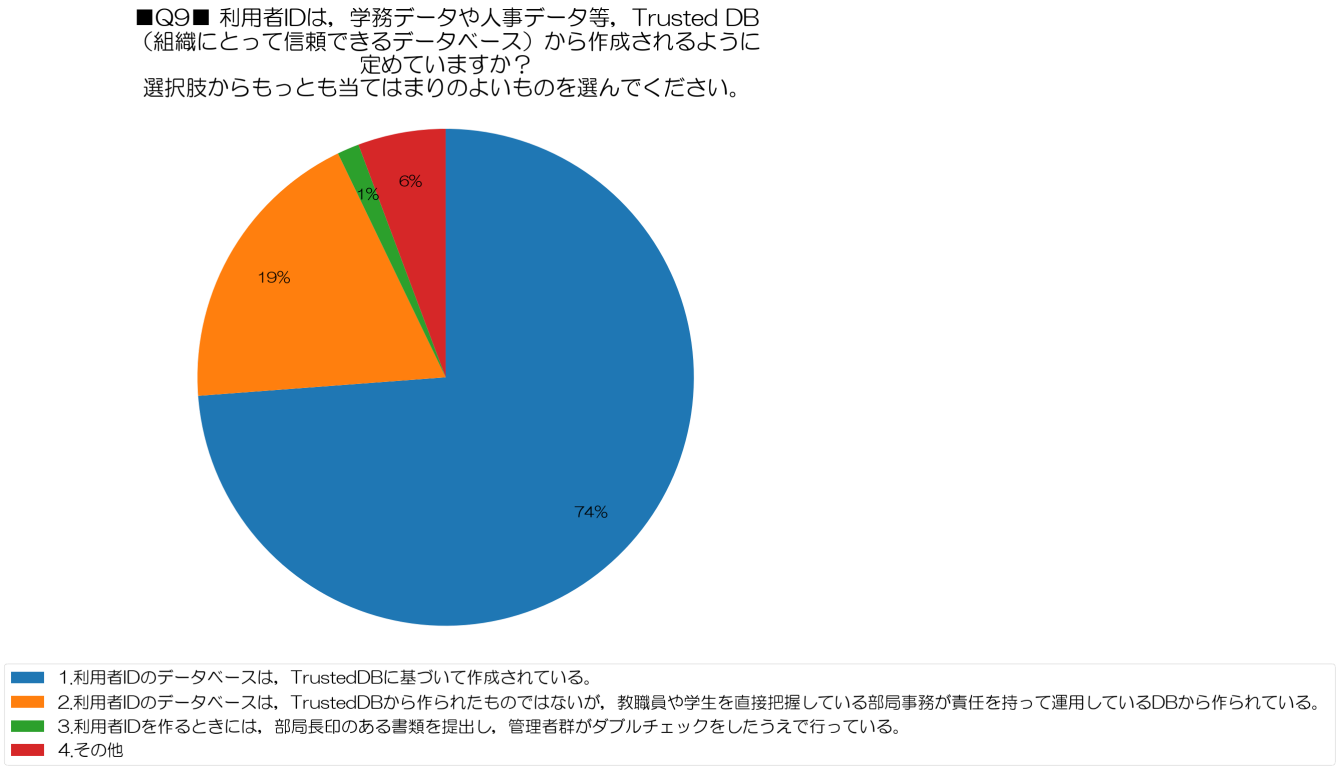
IDの運用状況（TRUSTED DB と直結しているかどうか）

利用者IDのソースとして、93%の機関でTrusted DBもしくは部局が責任をもって運用しているDBをもとにしており、適切なユーザ管理がなされていることが読み取れます(Q9)。また、「その他」との回答においても、構成員の一部からTrusted DBをもとにしたID管理に移行しつつあることが読み取られました。

上記以外の手法でのID管理は、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も増えていくという弱みを内包するものになります。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、事務フローや管理規則の整備をお勧めしたいと思います。

ゲスト/臨時アカウントについては、いくつかの機関において、前年度同様情報処理センター長の権限で発行できる体制があることが報告されました(Q10 自由記述)。記録を残す等、権限の適切な制御を併せてお願いしたいと思います。

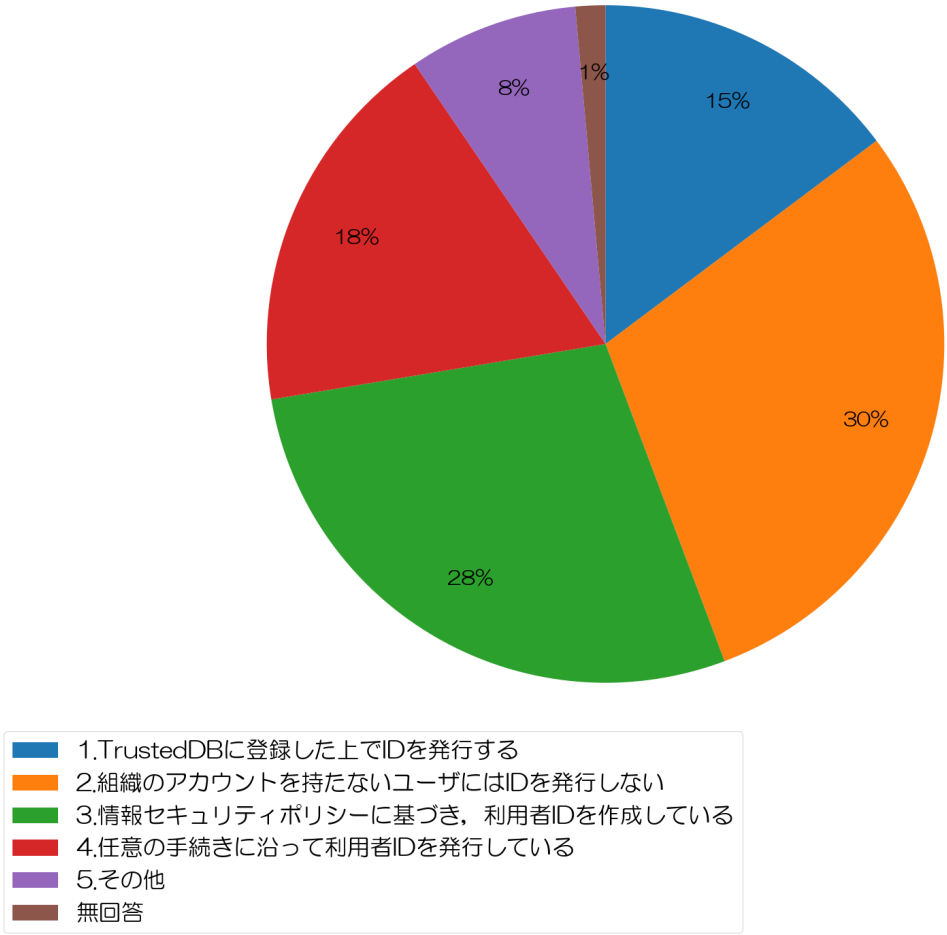
Q-9



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。	155
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。	40
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。	3
4. その他	12

Q-10

■Q10■ 前項（Q9）を踏まえ，Trusted DBに含まれないものから利用者IDを作成する場合，どのようなルールで作成されていますか？



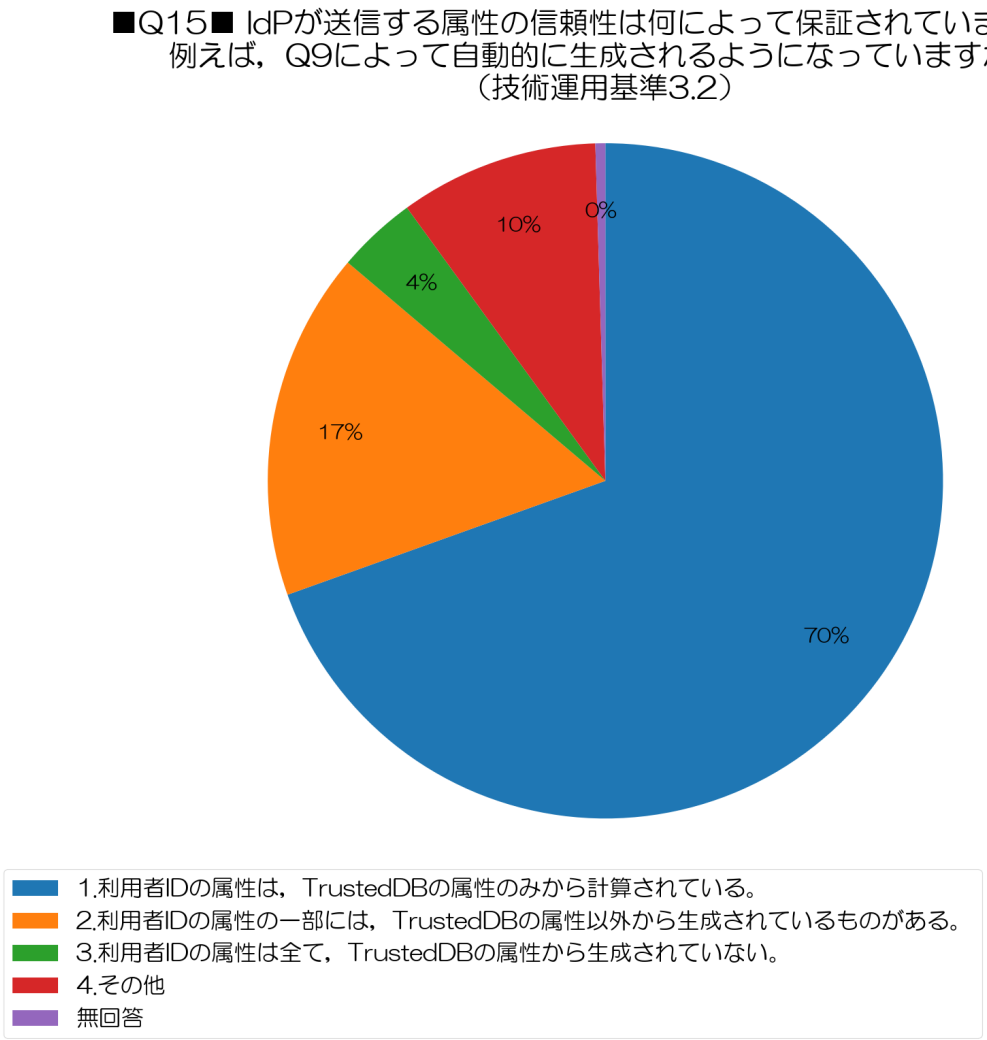
1. Trusted DBに登録した上でIDを発行する	31
2. 組織のアカウントを持たないユーザにはIDを発行しない	62
3. 情報セキュリティポリシーに基づき，利用者IDを作成している	59
4. 任意の手続きに沿って利用者IDを発行している	38
5. その他	17
無回答	3

属性保証

属性情報については、ほとんどの機関において、Trusted DBの属性のみから計算(Q15)されていたり、他組織の属性は付与しない体制（Q14自由記述より）となっており、システム運用基準3.2は正しく守られていると言えます。

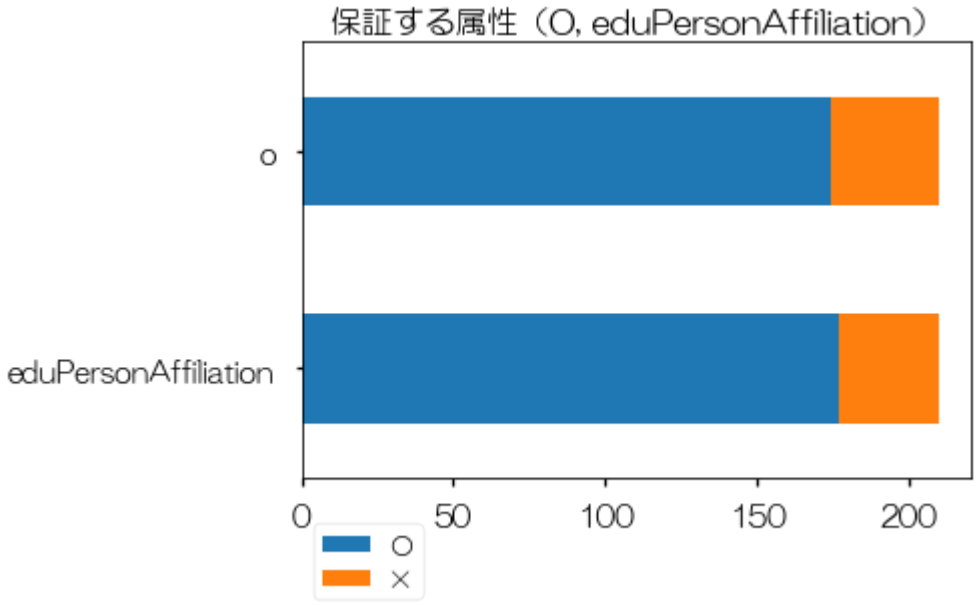
また今回も、前年度調査に引き続き、 o と eduPersonAffiliation の状況に着目しました。両属性は、80%以上の機関で組織として保証されていますが、「保証していない」としている機関がそれぞれ15%程度残っています。学認のIdPは機関ごとに設置して参加申請されており、機関名はIdPとして保証するべきです。送出できるよう設定してください。また実際にSPに送出し利用しているか否かにかかわらず、送出可能であれば「保証している」と回答してください。"faculty", "staff", "student", "member" など、利用者の職位を表すeduPersonAffiliationについても同様です。

Q-15



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。	146

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。	35
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。	8
4. その他	20
無回答	1



	○	×
o	174	36
eduPersonAffiliation	177	33

パスワードポリシー

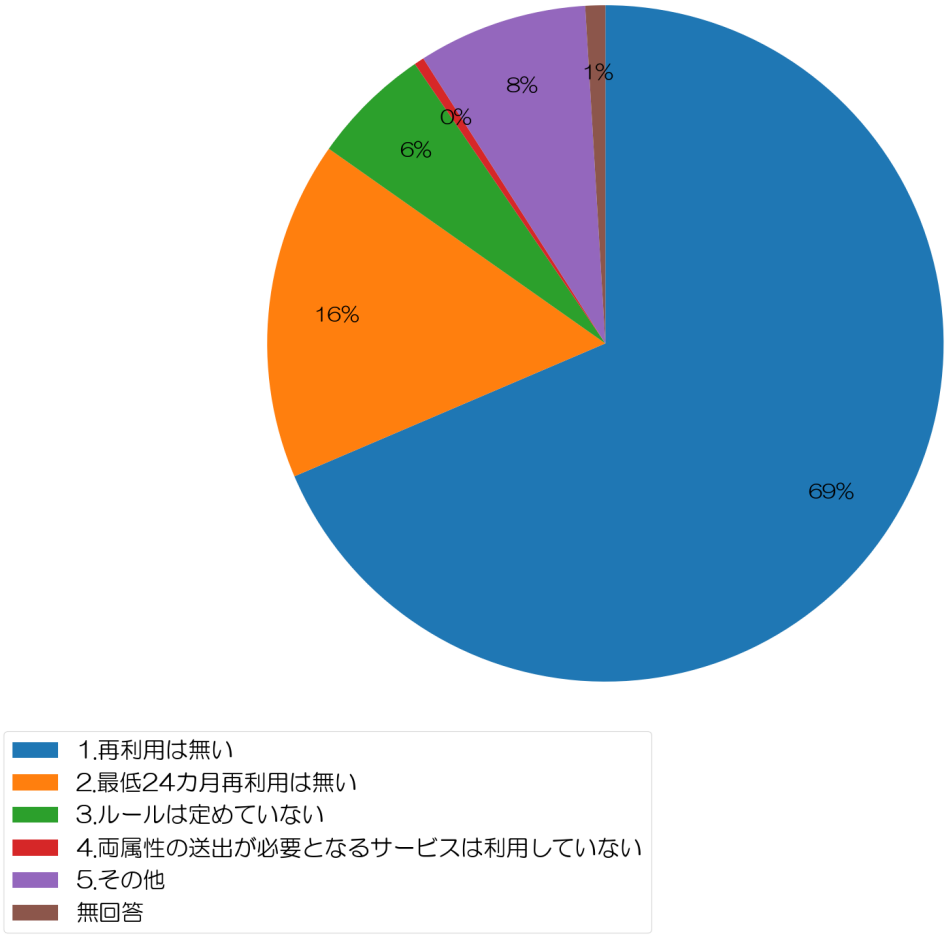
IDの再利用については、ごく少数のルールが定められていない機関を除き、再利用はないとの回答でした(Q19)。IDとクレデンシャルの配付については、本人確認を行うなど、各機関とも適切な運用が確立されています(Q20 自由記述より)。

共有IDの禁止に関しても、各機関にて、規定での禁止、セキュリティ面からの啓蒙活動や、共有しなくても業務を行えるような運用が行われていることが読み取れました(Q21 自由記述より)。

パスワードポリシーについては、93%の機関でパスワードポリシーがある、6%の機関でポリシーはないが啓蒙活動はしているとの回答でした(Q22)。

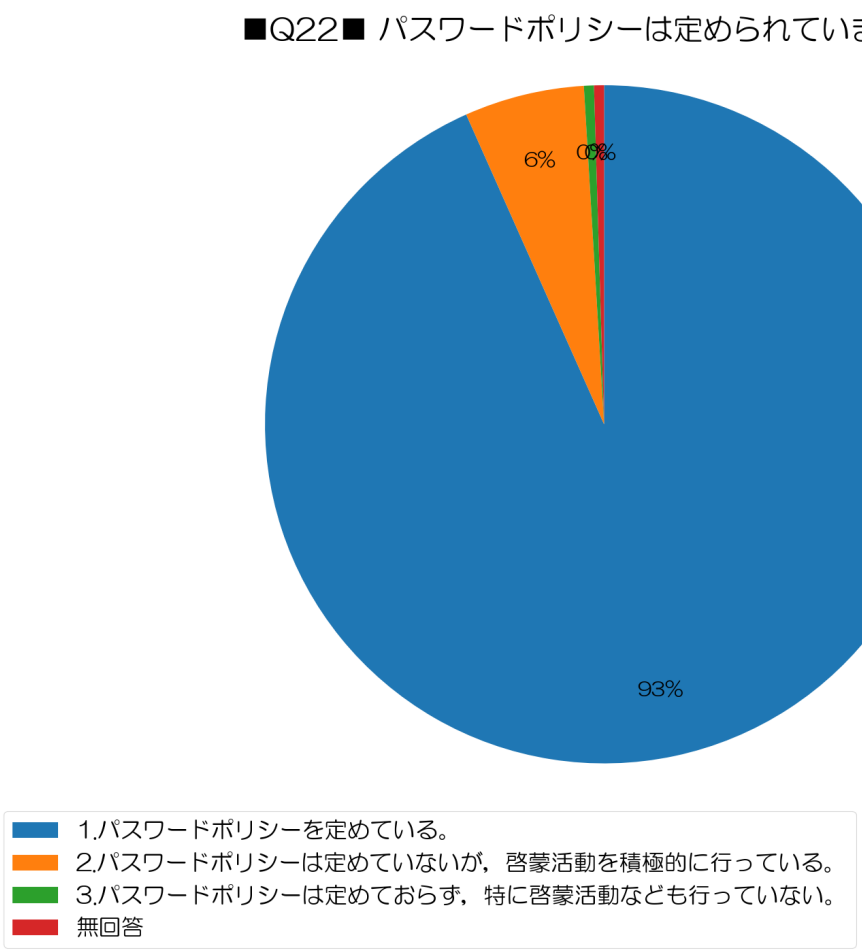
Q-19

■Q19■ eduPersonPrincipalNameとeduPersonTargetedIDに関しては，
かつて利用されていたものを再利用する場合は，
最終の利用時から最低24ヶ月間隔をあけることを定めています。
これを保証するために何が決められていますか？
（技術運用基準8.2）



1. 再利用は無い	144
2. 最低24カ月再利用は無い	34
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	1
5. その他	17
無回答	2

Q-22



1. パスワードポリシーを定めている。	196
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。	12
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
無回答	1

その他

ログの保存期間については、多くの大学が最低3か月から1年以上保存する運用となっています。学認技術運用基準にて推奨する3か月より短い保存期間を設定している機関はありませんでしたが、「定められていない」との回答がまだ一部みられます。3ヶ月以上の最低保存期間を定めていただきたいと思います(Q29 自由記述より)。

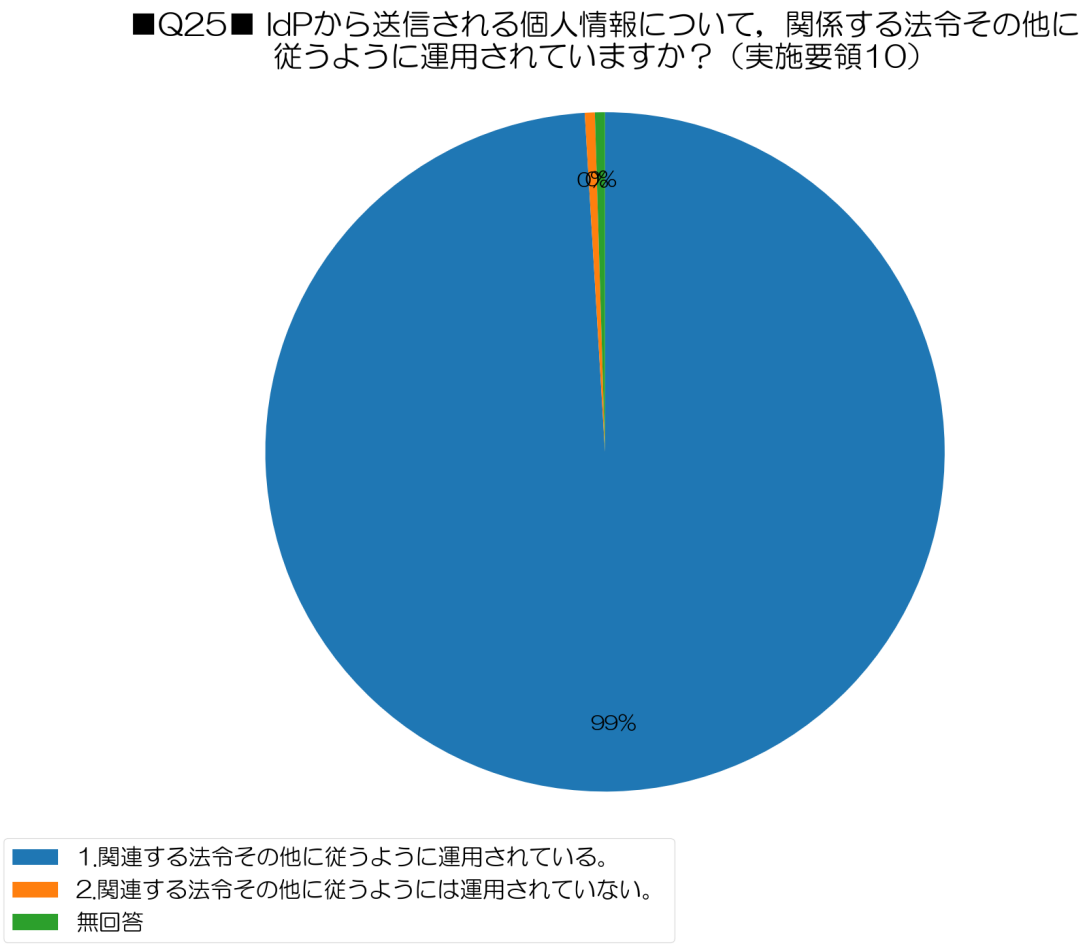
4 プライバシー（プライバシーに関係すること）

IdPから送信される個人情報については、2件を除き、関係する法令に従うように運用されていいます(Q25)。「関連する法令その他に従うようには運用されていない」と回答した1件は、「まだ全学での本格運用が始まっていないため」との連絡を学認事務局が受けています。適法でない運用状態が放置されているということではありません。

また、プライバシーについて具体的な規則を制定している機関は前年から微増の60%程度(Q26)、uApproveもしくはShibboleth IdP Version 3で搭載された属性リリース同意取得機能を利用していると回答した機関は139件（約66%）でした(Q27)。

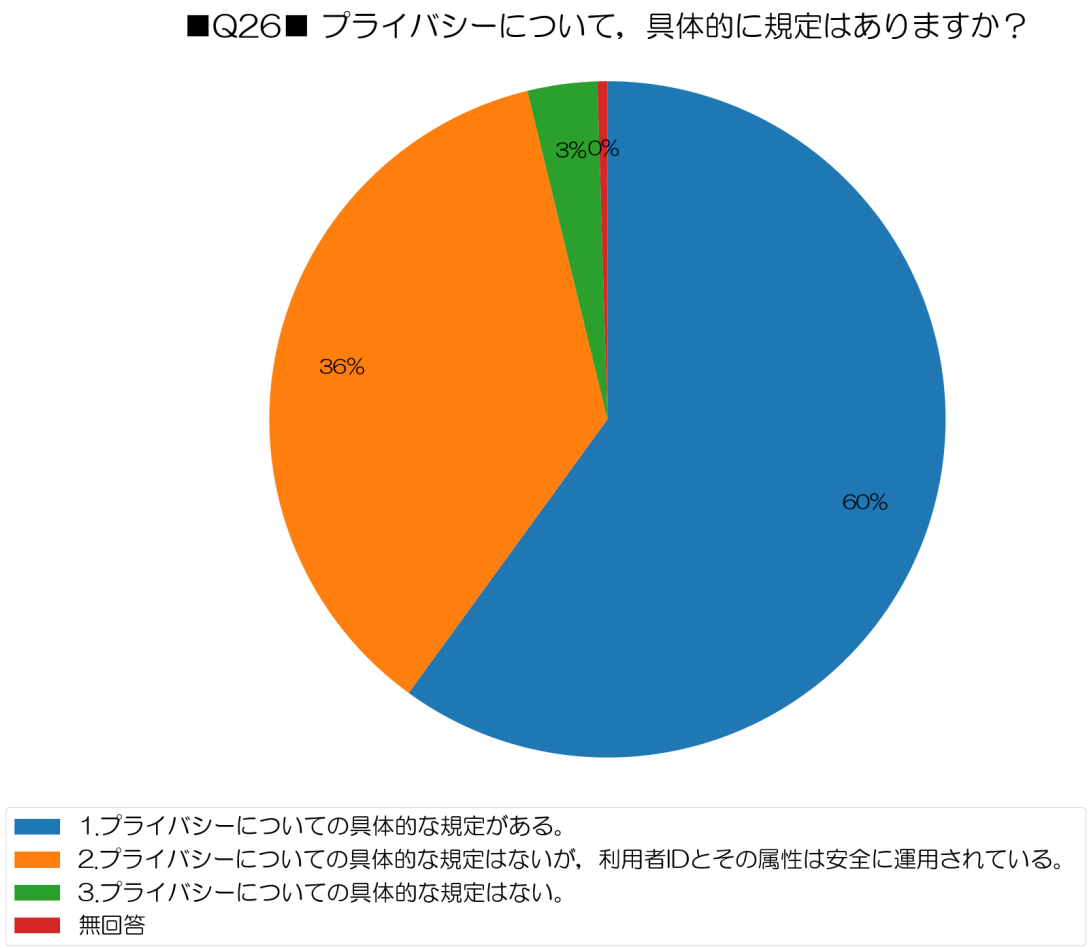
個人情報保護については、いずれも前年とほぼ同水準を維持していました。

Q-25



1. 関連する法令その他に従うように運用されている。	208
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。	1
無回答	1

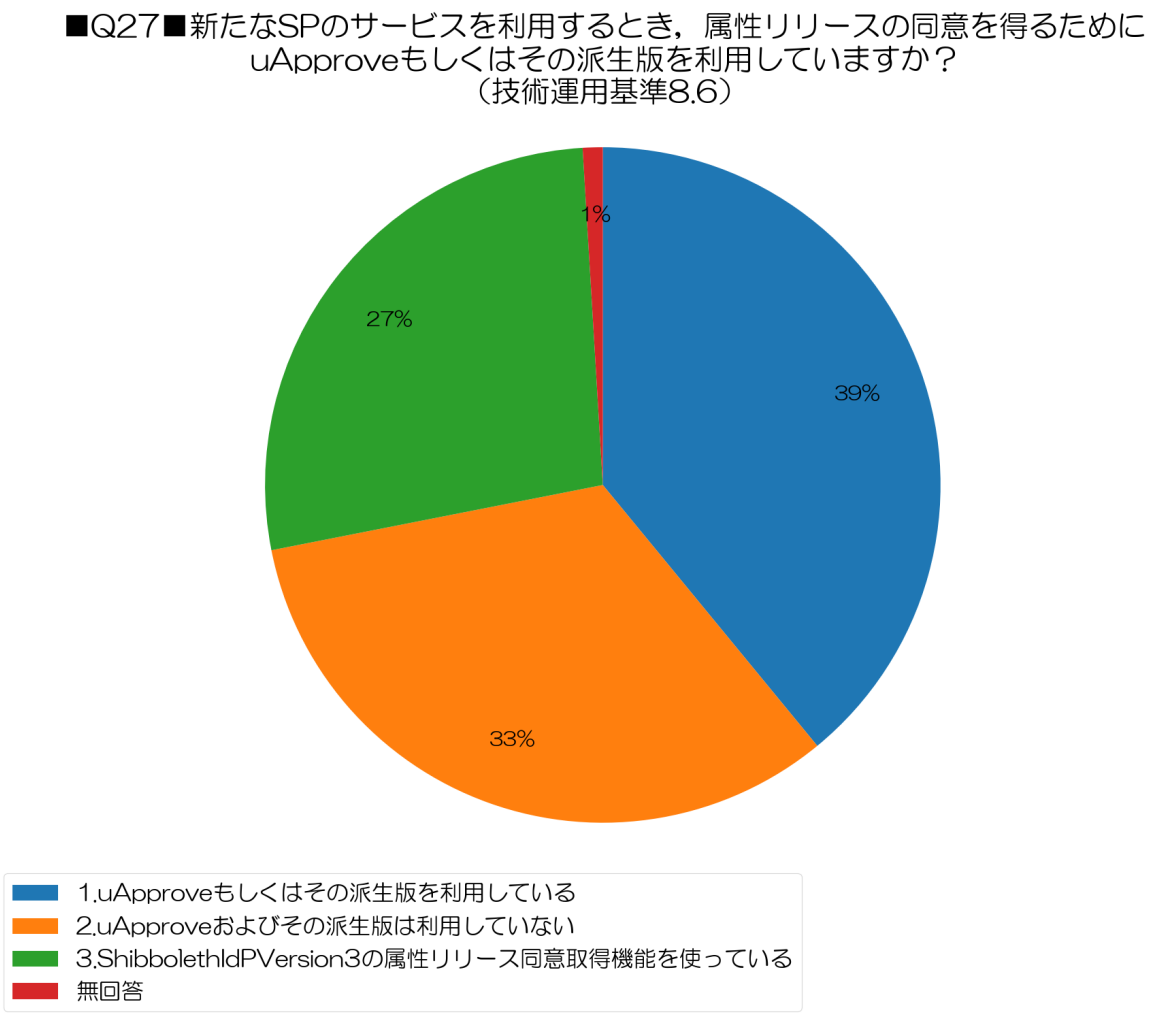
Q-26



1. プライバシーについての具体的な規定がある。	126
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。	76
3. プライバシーについての具体的な規定はない。	7

無回答	2

Q-27



1. uApproveもしくはその派生版を利用している	82
2. uApproveおよびその派生版は利用していない	69
3. Shibboleth IdP Version3の属性リリース同意取得機能を使っている	57
4. IDaaSに組み込まれている属性リリース同意取得機能を使っている	0
無回答	2

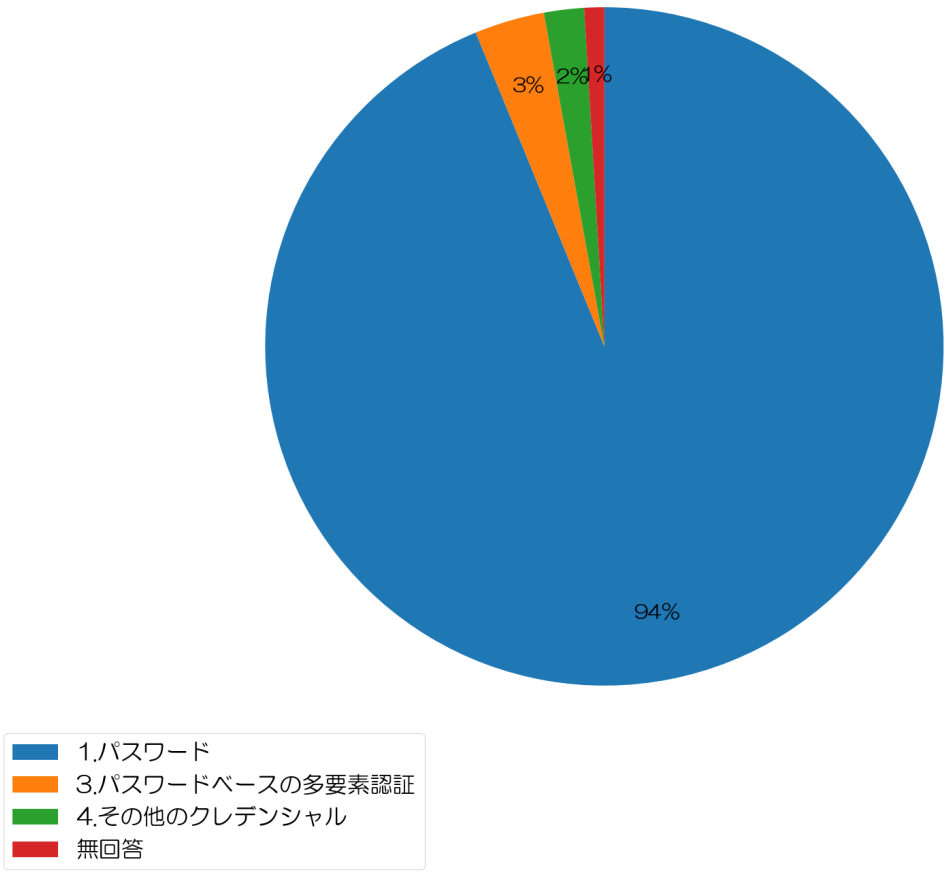
5 利用者IDのクレデンシャル

利用者IDとして利用している主なクレデンシャルの種類（Q38）としては、そのほとんど、94%がパスワードであるとの回答でした。また電子証明書による認証や、パスワードベースの多要素認証が導入されています。「4.その他のクレデンシャル」との回答には補足として自由記述欄が付与されていますが、そこには一部の成員で電子証明書を用いた認証や、FeliCaなどのICカードによる認証、マトリクス認証を行っていると記述されていました。準備段階ながら、SNSと連携した認証の導入も進められているとのことです。

Q44は、クレデンシャルの安全性を実現するために実施している取り組みについて質問したものです。現状の把握を目的としたものですが、設問中のいくつかは、NIST SP800-63-3において、非推奨とされているものがあります。無論、ここで○と回答したものが誤りであるということではなく、現在、機関で定められている規程類に該当する記述がある場合、それは守られるべきものです。注視すべきは、策定時には正しいとされていたものが、取り巻く制度的、あるいは技術的状況によって変化していく可能性があるという点です。規程類は一度定めたらそれでよいものではなく、継続的なメンテナンスを行っていく必要があるものだということを、ご認識いただきたいと思います。

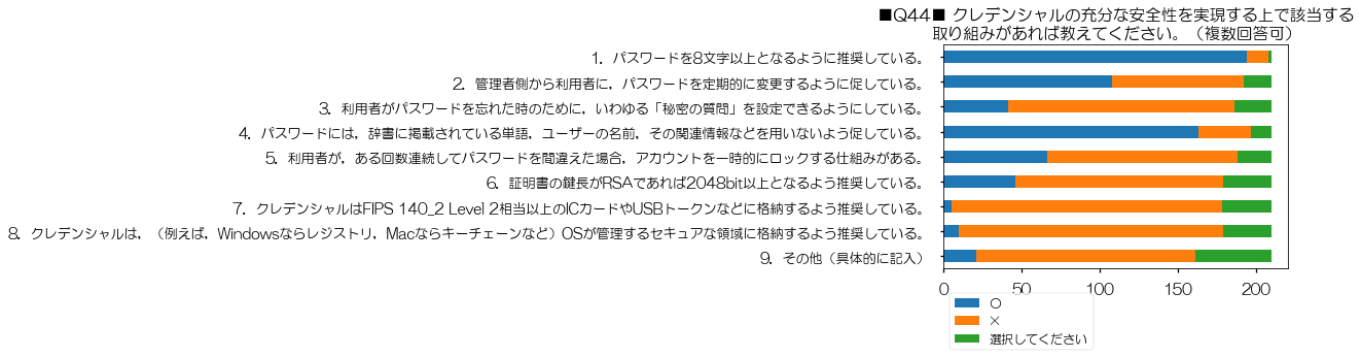
Q-38

■Q38■ 利用者IDとして利用している主なクレデンシャルの種類を教えてください。
利用者IDの種類によって異なるクレデンシャルを利用している場合，
もしくは同一ID種で複数のクレデンシャルを利用している場合は，
主要な利用者ID種および主要なクレデンシャルについて選んでいただいた上で，
他のクレデンシャルについては補足事項欄にて補足してください。



1. パスワード	197
3. パスワードベースの多要素認証	7
4. その他のクレデンシャル	4
無回答	2

Q-44



	○	×	選択してください
1. パスワードを8文字以上となるように推奨している。	194	14	2
2. 管理者側から利用者に，パスワードを定期的に変更するように促している。	108	84	18
3. 利用者がパスワードを忘れた時のために，いわゆる「秘密の質問」を設定できるようにしている。	41	145	24
4. パスワードには，辞書に掲載されている単語，ユーザーの名前，その関連情報などを用いないよう促している。	163	34	13
5. 利用者が，ある回数連続してパスワードを間違えた場合，アカウントを一時的にロックする仕組みがある。	66	122	22
6. 証明書の鍵長がRSAであれば2048bit以上となるよう推奨している。	46	133	31
7. クレデンシャルはFIPS 140_2 Level 2相当以上のICカードやUSBトークンなどに格納するよう推奨している。	5	173	32
8. クレデンシャルは，（例えば，Windowsならレジストリ，Macならキーチェーンなど）OSが管理するセキュアな領域に格納するよう推奨している。	10	169	31
9. その他（具体的に記入）	21	140	49

6 IDPの設定・運用管理

ここからは、IdPの設定と運用管理について、主に技術的な側面からの設問となります。設定ファイルの管理、稼働するミドルウェア群のアップデート状況、そしてサポートが終了したShibboleth IdP version 2系統から3系統へのアップグレード状況について質問しています。

まず設定ファイルの管理（Q32）は、機関内での管理が131件（62%）、設定変更を都度外部に依頼しているとしたものが71件（34%）と、どちらも前年とほぼ同等の割合でした。IdPの設定ファイルは適切な管理（現状の最新版はどれで、現在IdPに反映されているものはどれか？など）と設定変更が行えるようになっていれば問題はありません。IDaaSでの管理も同様です。管理体制が不明という回答が1件だけありましたが、これは通常ありえることではありません。IdPの運用管理部局に確認するなどして、適切な取り扱いができるよう、管理体制を明確にしておく必要があるでしょう。

Q48は、学認事務局からお知らせしている、Shibbolethの稼働に必要なミドルウェア群の脆弱性情報への対応状況を質問したものです。総じて8割程度の機関で、アップデート済みもしくは年度内に対応予定とされています。多くの機関で対応いただけている状況が見られます。一方、対応状況が不明であるとの回答が一定数あります。ソフトウェアの既知の脆弱性を突かれ、情報漏洩につながった事例が何件も報道されており、対応の遅れが甚大な被害につながるケースを目にしたことと思います。IdPに限らないことですが、管理下にあるサーバで稼働するソフトウェア群のバージョンやアップデート状況を把握できるよう努めていただきたいと思います。

なお学認事務局からは、Shibbolethとその動作に関連したミドルウェアについての情報提供のみを実施しており、それ以外の脆弱性等については提供しておりません。管理対象が多すぎて手が回らない、といった状況にあるなら、脆弱性スキャナーを用いたチェックの自動化をご検討ください。

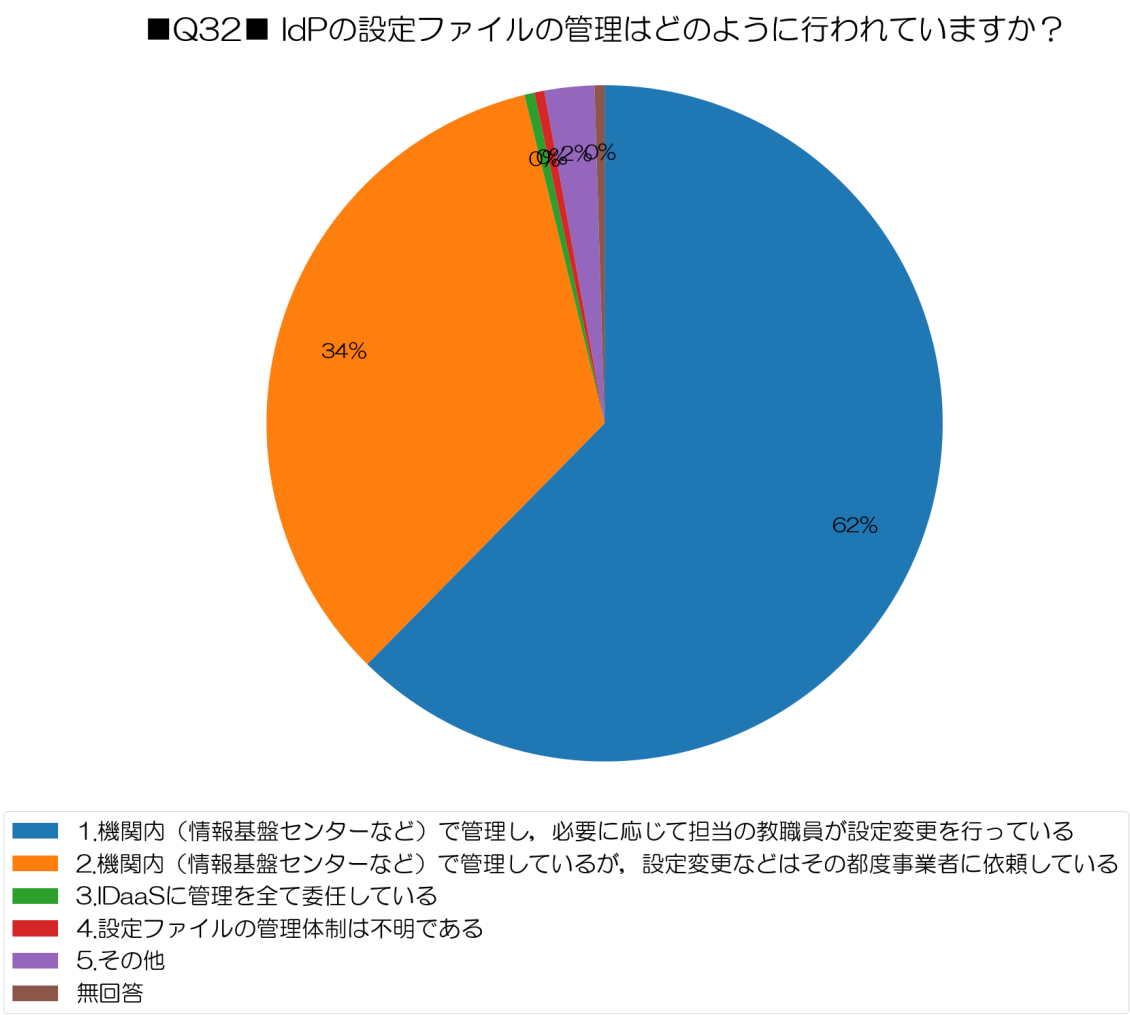
また、長期的にみて、脆弱性のアナウンス件数は増加傾向にあります。調査実施以降も、学認事務局よりご案内してきました。事務局からの情報に、引き続き注視していただきたいと思います。

Q49は、調査実施時点ですでにサポートが終了していた、Shibboleth IdP version 2系統から、現行のVersion3系統へのアップグレード状況についての質問です。調査実施時点でもまだ、11のIdPでversion2系統が稼働しています。

当然の話ですが、サポートが終了したソフトウェアを使い続けることは望ましくありません。Shibboleth IdP version 2 においては、もうアップデートは提供されないと明言されていますし、学認事務からの技術情報はVersion3のみで提供しております。

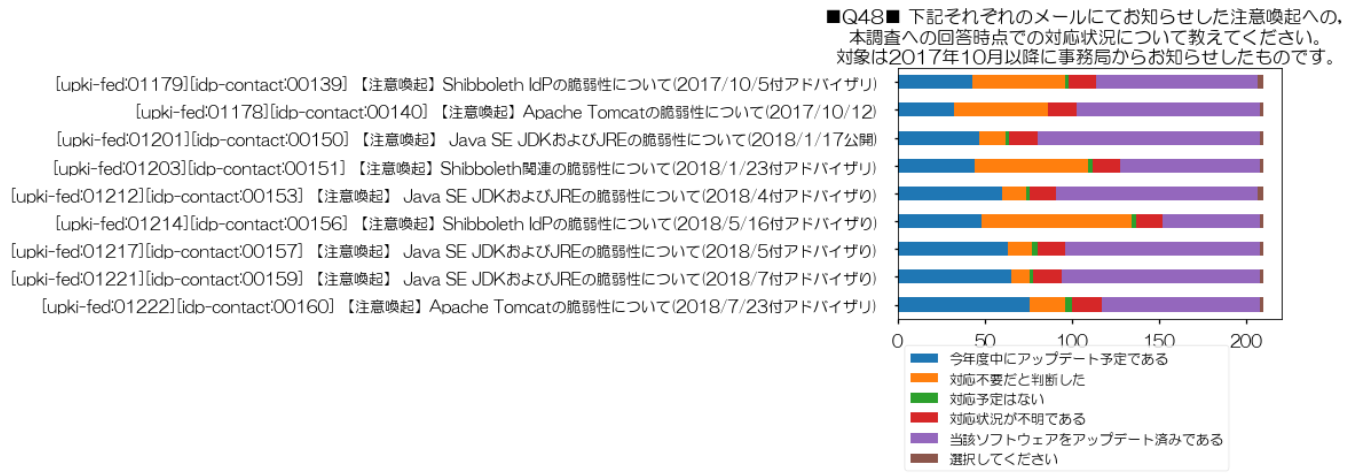
アップグレードが完了していない機関、アップグレード予定はないと回答した機関は、こうした状況を鑑み、是非アップグレードを実施してください。

Q-32



1. 機関内（情報基盤センターなど）で管理し，必要に応じて担当の教職員が設定変更を行っている	131
2. 機関内（情報基盤センターなど）で管理しているが，設定変更などはその都度事業者に依頼している	71
3. IDaaSに管理を全て委任している	1
4. 設定ファイルの管理体制は不明である	1
5. その他	5
無回答	1

Q-48

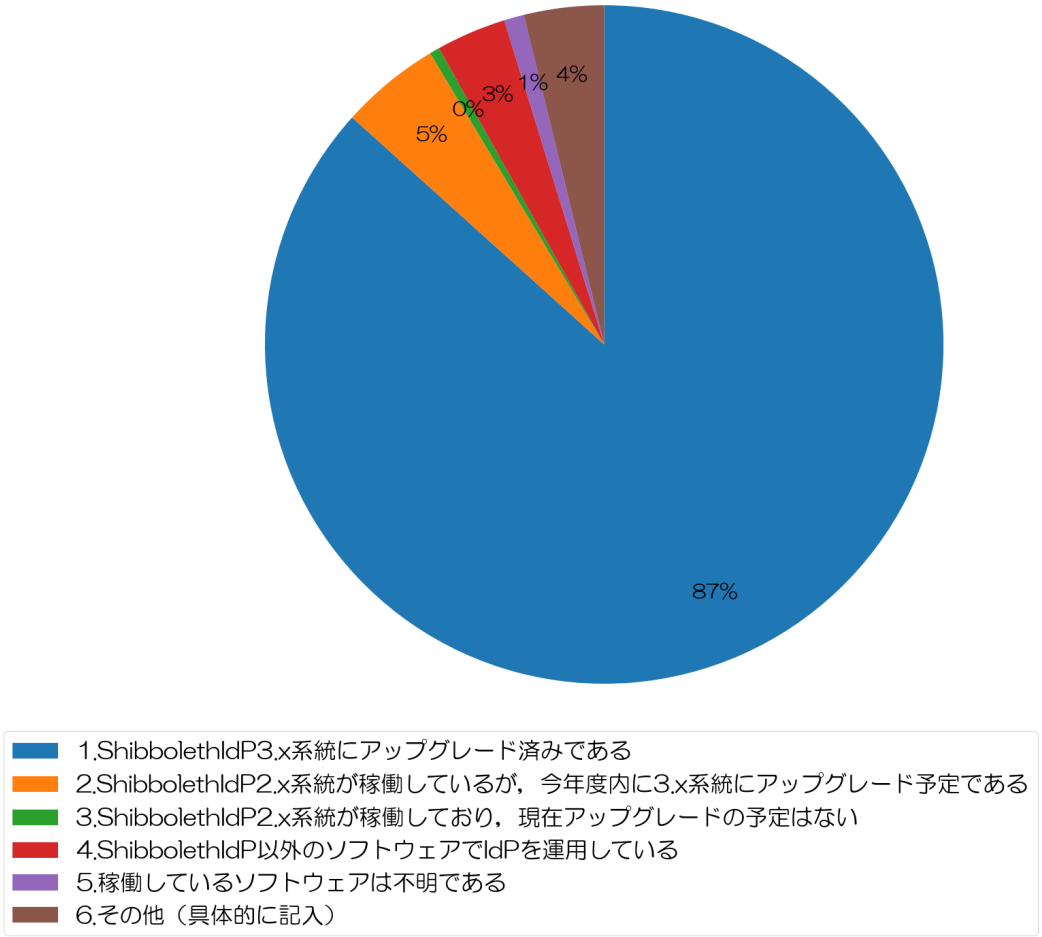


	今年度中にアップデート予定である	対応不要だと判断した	対応予定はない	対応状況が不明である	当該ソフトウェアをアップデート済みである	選択してください
[upki-fed:01179][idp-contact:00139] 【注意喚起】 Shibboleth IdPの脆弱性について (2017/10/5付アドバイザリ)	43	53	2	16	93	3
[upki-fed:01178][idp-contact:00140] 【注意喚起】 Apache Tomcatの脆弱性について (2017/10/12)	32	54	0	17	105	2
[upki-fed:01201][idp-contact:00150] 【注意喚起】 Java SE JDKおよびJREの脆弱性について (2018/1/17公開)	47	15	2	16	128	2
[upki-fed:01203][idp-contact:00151] 【注意喚起】 Shibboleth関連の脆弱性について (2018/1/23付アドバイザリ)	44	65	3	16	80	2
[upki-fed:01212][idp-contact:00153] 【注意喚起】 Java SE JDKおよびJREの脆弱性について (2018/4付アドバイザリ)	60	14	2	15	116	3

[upki-fed:01214][idp-contact:00156] 【注意喚起】 Shibboleth IdPの脆弱性について (2018/5/16付アドバイザり)	48	86	3	15	56	2
[upki-fed:01217][idp-contact:00157] 【注意喚起】 Java SE JDKおよびJREの脆弱性について (2018/5付アドバイザり)	63	14	3	16	112	2
[upki-fed:01221][idp-contact:00159] 【注意喚起】 Java SE JDKおよびJREの脆弱性について (2018/7付アドバイザり)	65	11	2	16	114	2
[upki-fed:01222][idp-contact:00160] 【注意喚起】 Apache Tomcatの脆弱性について (2018/7/23付アドバイザリ)	76	20	4	17	91	2

Q-49

■Q49■ すでにお知らせしている通り，Shibboleth IdP 2.x系はサポートが終了しております。
現在稼働しているIdPのソフトウェアの状況について教えてください。



1. Shibboleth IdP 3.x系統にアップグレード済みである	182
2. Shibboleth IdP 2.x系統が稼働しているが，今年度内に3.x系統にアップグレード予定である	10
3. Shibboleth IdP 2.x系統が稼働しており，現在アップグレードの予定はない	1
4. Shibboleth IdP 以外のソフトウェアでIdPを運用している	7
5. 稼働しているソフトウェアは不明である	2
6. その他（具体的に記入）	8

本調査にご協力いただき、ありがとうございました。