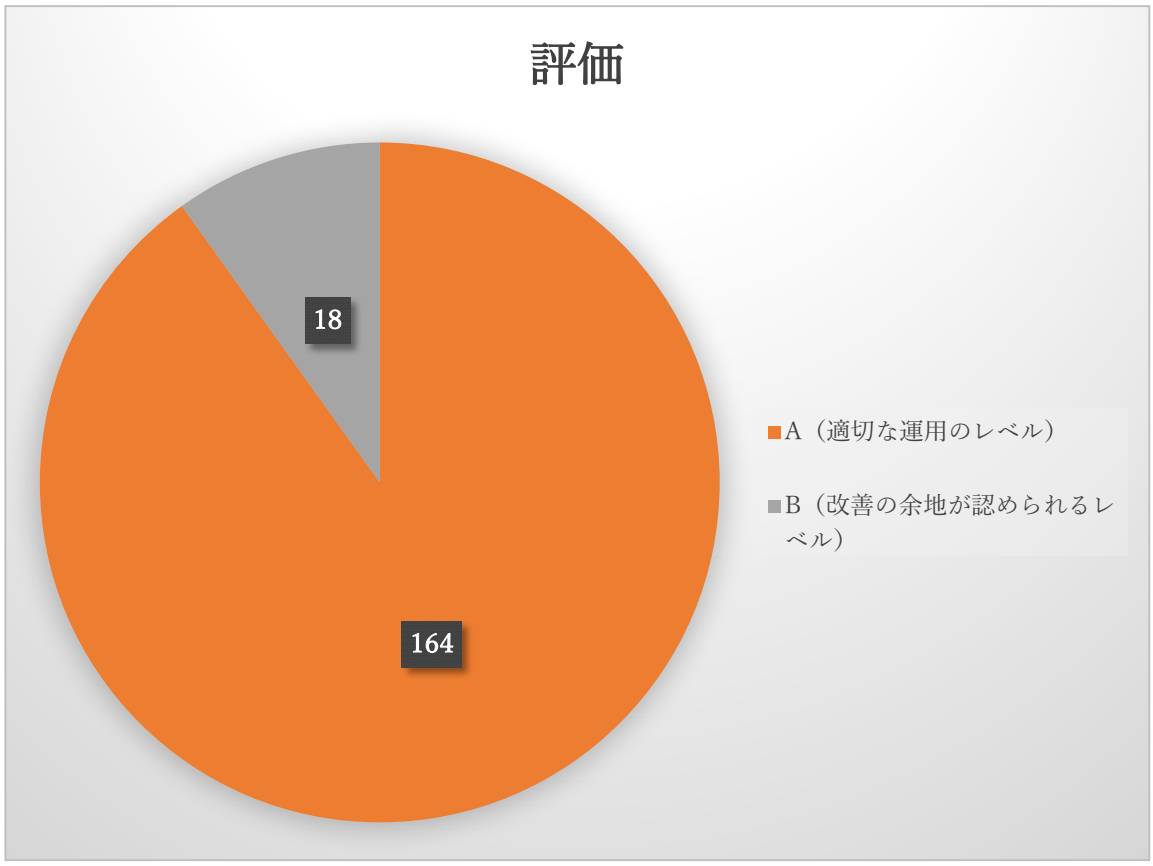
平成 29 年 8 月 3 日

トラスト作業部会

2016 年度
学認参加 IdP 運用状況調査報告

1　評価結果

アンケート回答機関数は 182 件(100%)です。適切な運用を行っている機関が 164 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 18 件みられました。



本調査の評価は、下記の 2015 年評価基準を引き継いでいます。

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

これらの基準に加え、2016 年の調査では下記の基準を追加しました。

1. 設定ファイルの管理体制について
2. 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
3. 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。

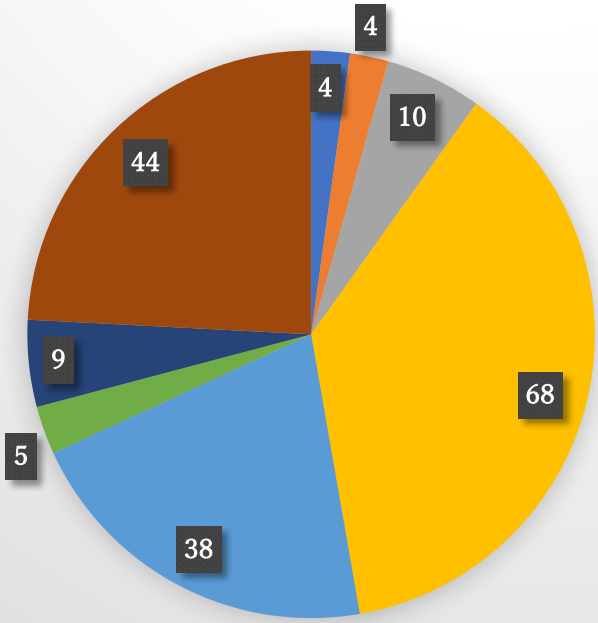
総じて前年度調査に続き、高い水準で IdP が運用されていたことが読み取れました。また、前年度 B 評価だった機関は、半数以上が今回の調査で A 評価を取得しています。学認参加の各機関には、引き続きの運用をお願いいたします。

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、161 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 18 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 71 件（39％）が定められているとの回答でした(Q31)。

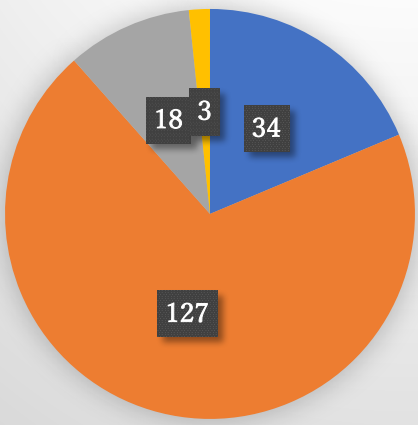
多くの機関において、利用者 ID の管理体制や全学的なセキュリティポリシーが整備されています。その基盤の上になりたって IdP が適切に運用されていることが読み取れます。Q8 において、なんらかの規程が整備されているとの回答は 86 件ですが、その他 44 件の自由記述の内容を読んでいくと、規程の整備状況をより丁寧に説明したものが多く見られました。前年度調査の結果に続き、半数以上の機関で整備されていると読み取ることができます。

Q8:IdP運用上での根拠規則や内規の制定状況について

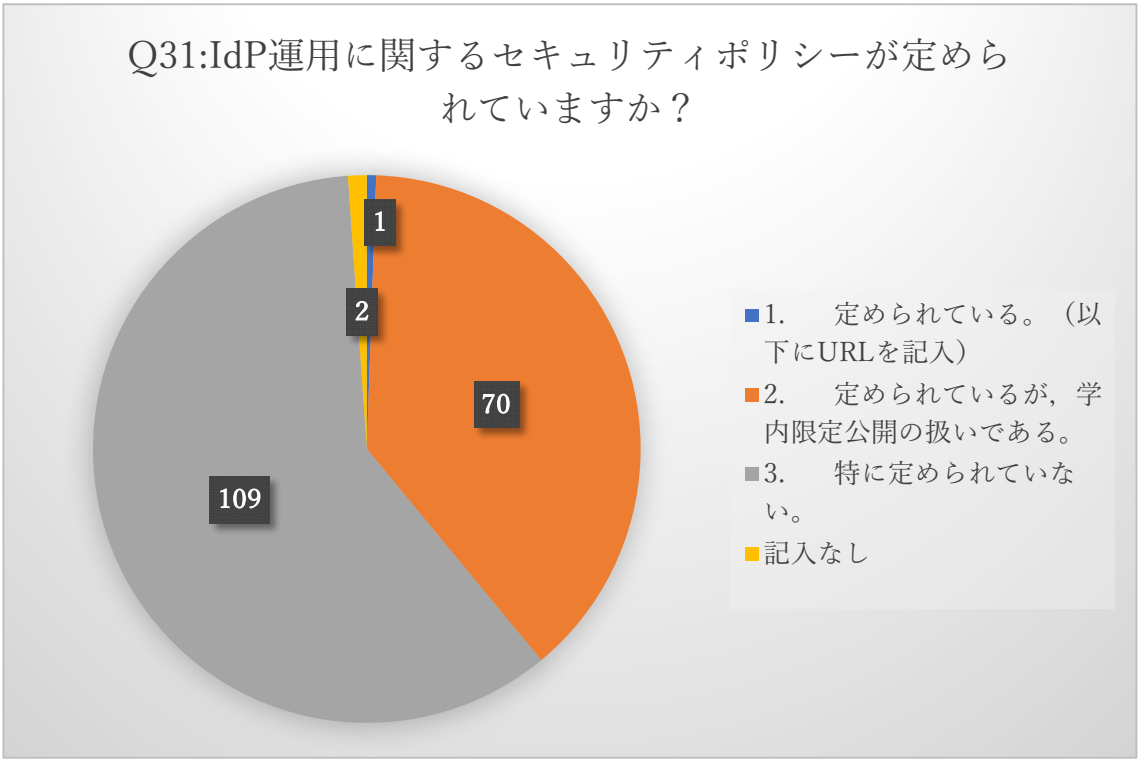


- 1. 全学情報サービスを担当する情報基盤センターの内規がある。【URLを記入】
- 2. IdP運用規則，全学サービスセキュリティポリシーがある。【URLを記入】
- 3. IdP運用規則，全学サービスセキュリティポリシーがあり，学内限定で公開されている。
- 4. 全学サービスセキュリティポリシーが存在する。IdPはそのもとで適切に運用されている。
- 5. 特にないが，運用責任者の管理の下，適切に運用されている。
- 6. 規則などは特にないが，現在制定中である。
- 7. 全学的にはテスト利用の扱いになっている。
- 8. その他

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）
- 2. 定められているが，学内限定公開の扱いである。
- 3. 特に定められていない。
- 記入なし



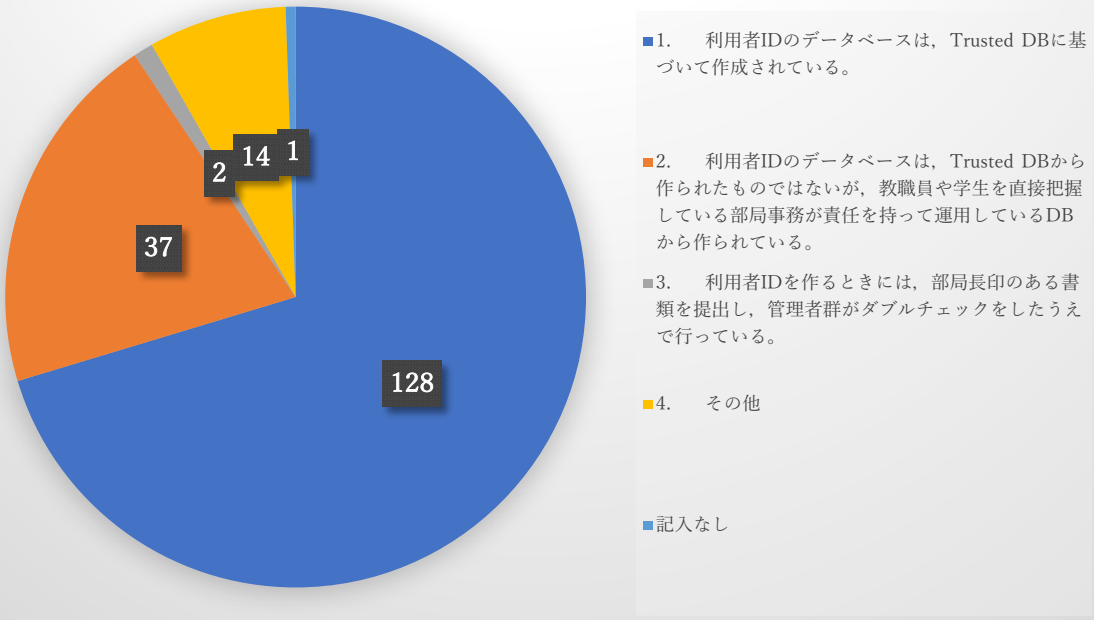
3 テクニカルなこと

ID の運用状況（Trusted DB と直結しているかどうか）

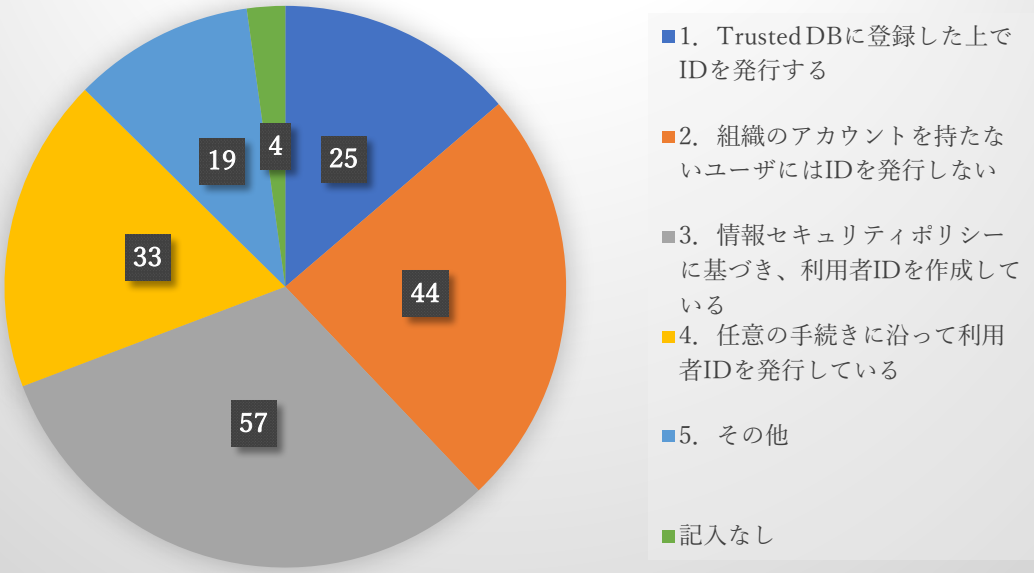
今年度を含むここ 3 年間の調査において、利用者 ID のソースとしては、一部の機関を除き、Trusted DB もしくは部局が責任をもって運用している DB をもとにしており、適切なユーザ管理がなされていることが読み取れます(Q9)。一方、それ以外の手法での ID 管理は、今後の ID 数の増加、保持させる属性情報の増加に比例してその手間も増えていくという弱みを内包するものになります。スケーラビリティの観点から、ID 管理を Trusted DB に直結する形で行えるよう、事務フローや管理規則の整備をお勧めしたいと思います。

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。

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ますか？ 選択肢からもっとも当てはまりのよいものを選んでください。



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。

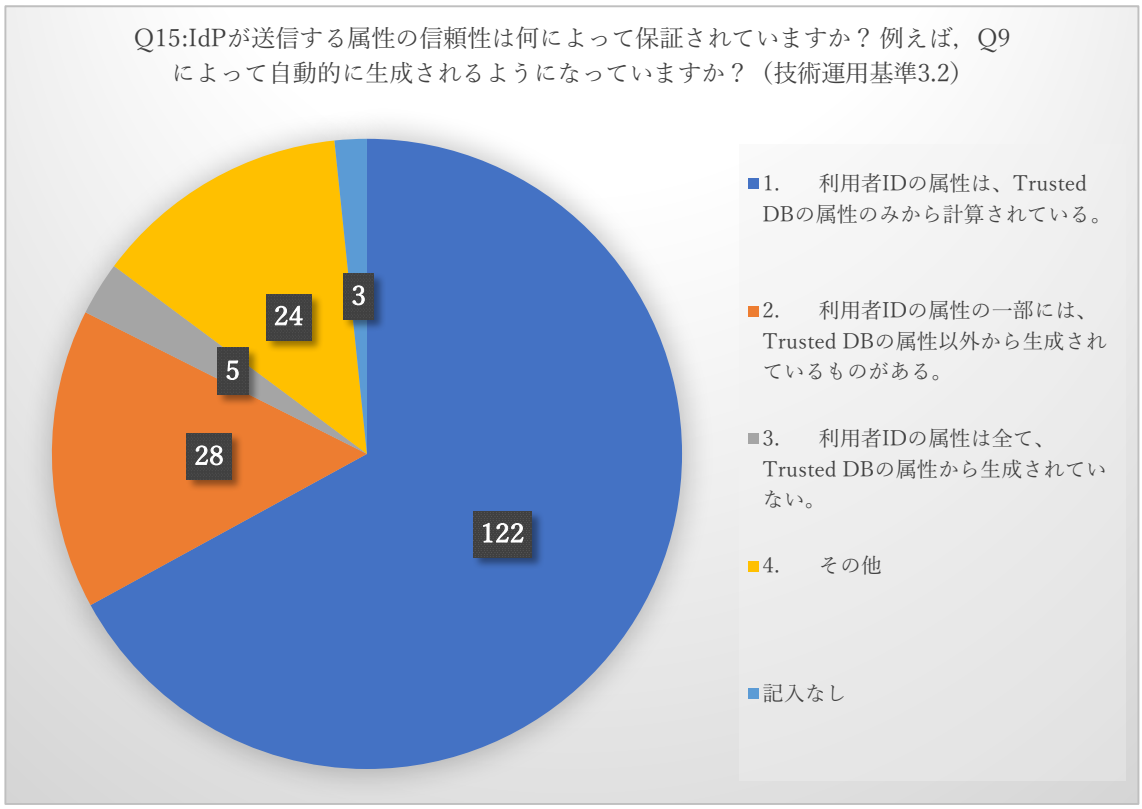


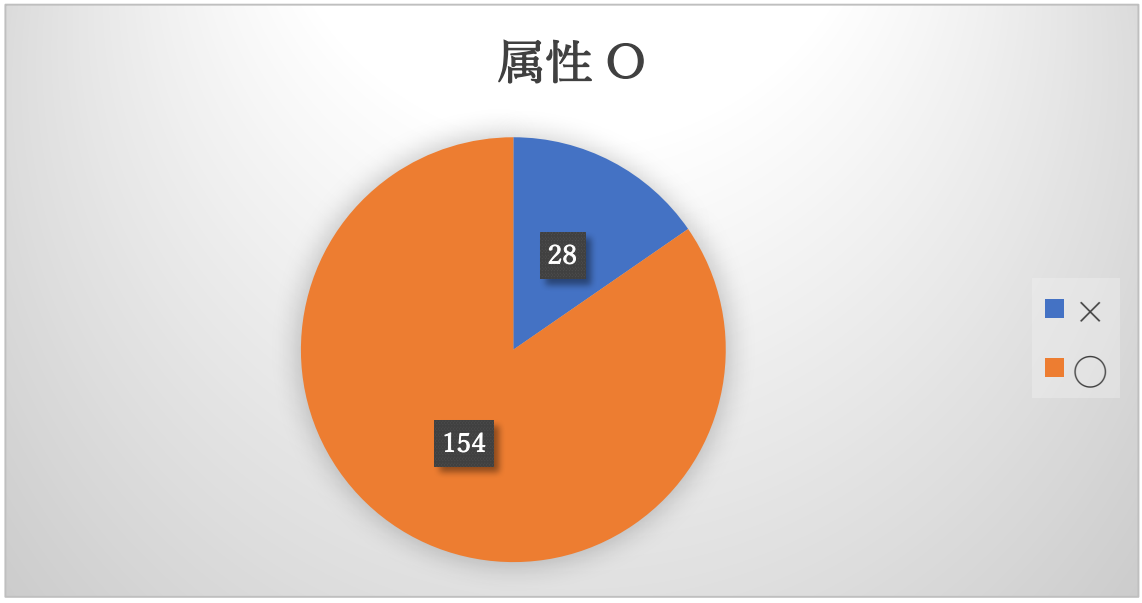
属性保証

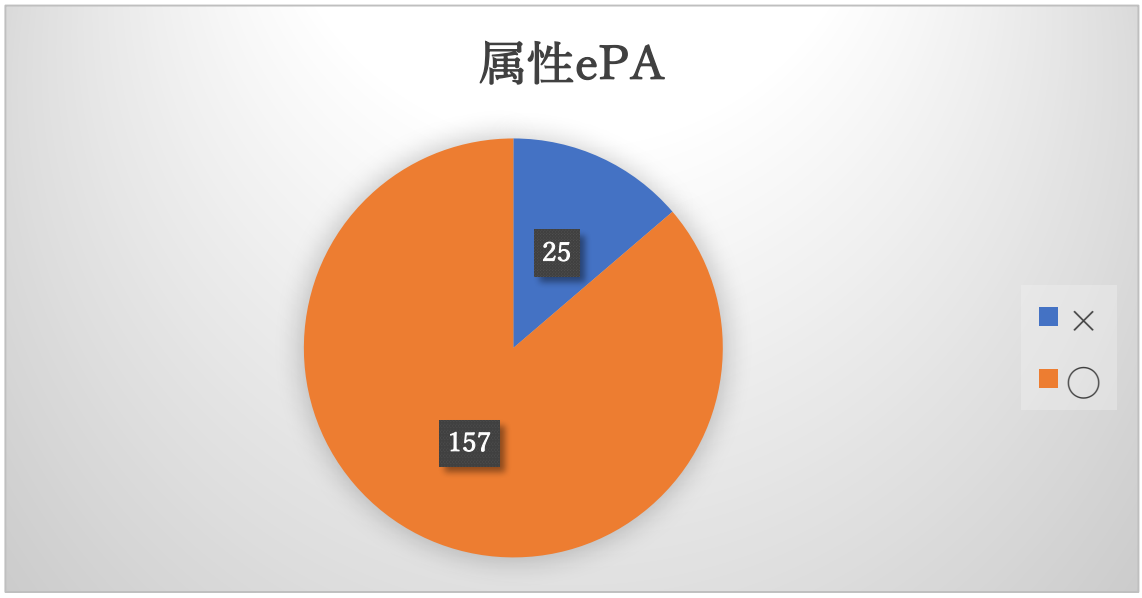
属性情報については、ほとんどの機関において、Trusted DB の属性のみから計算や、他組織の属性は付与しない体制となっており、システム運用基準 3.2 は正しく守られています(Q15)。

今回も、前年度調査に引き続き、 o と eduPersonAffiliation 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。

前年度同様、この両者を保証していない機関が B と判定されたケースが多かったことを附言しておきます。





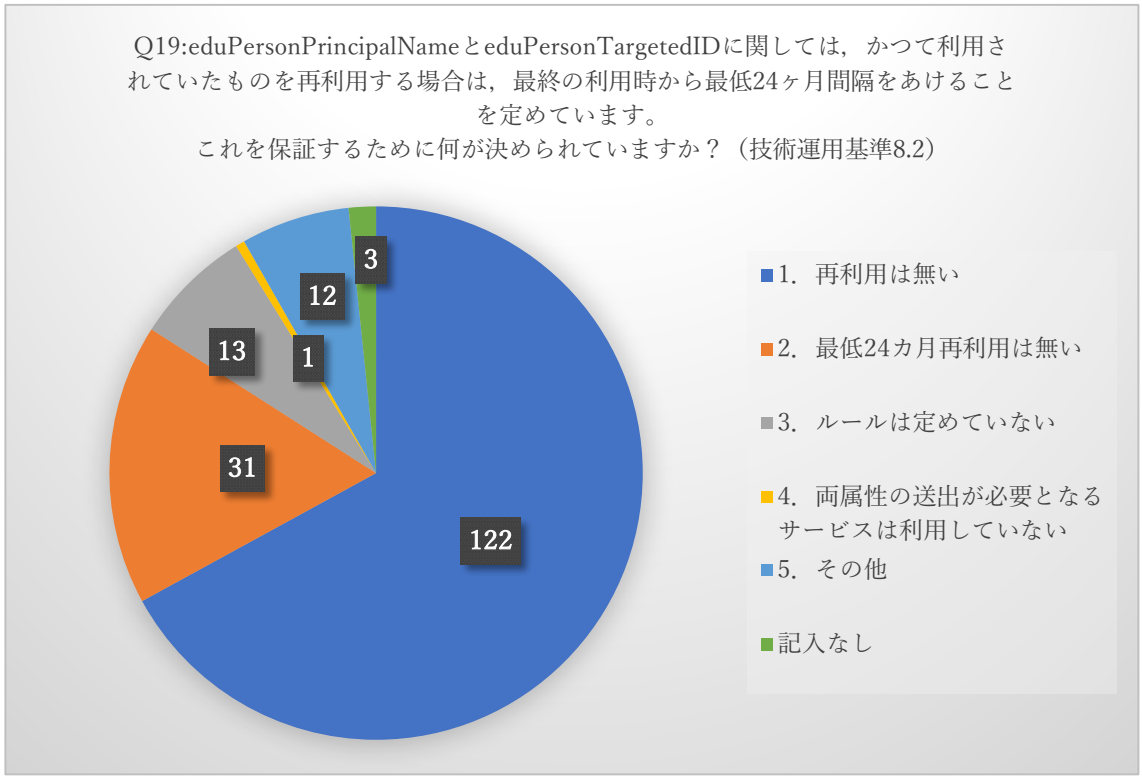


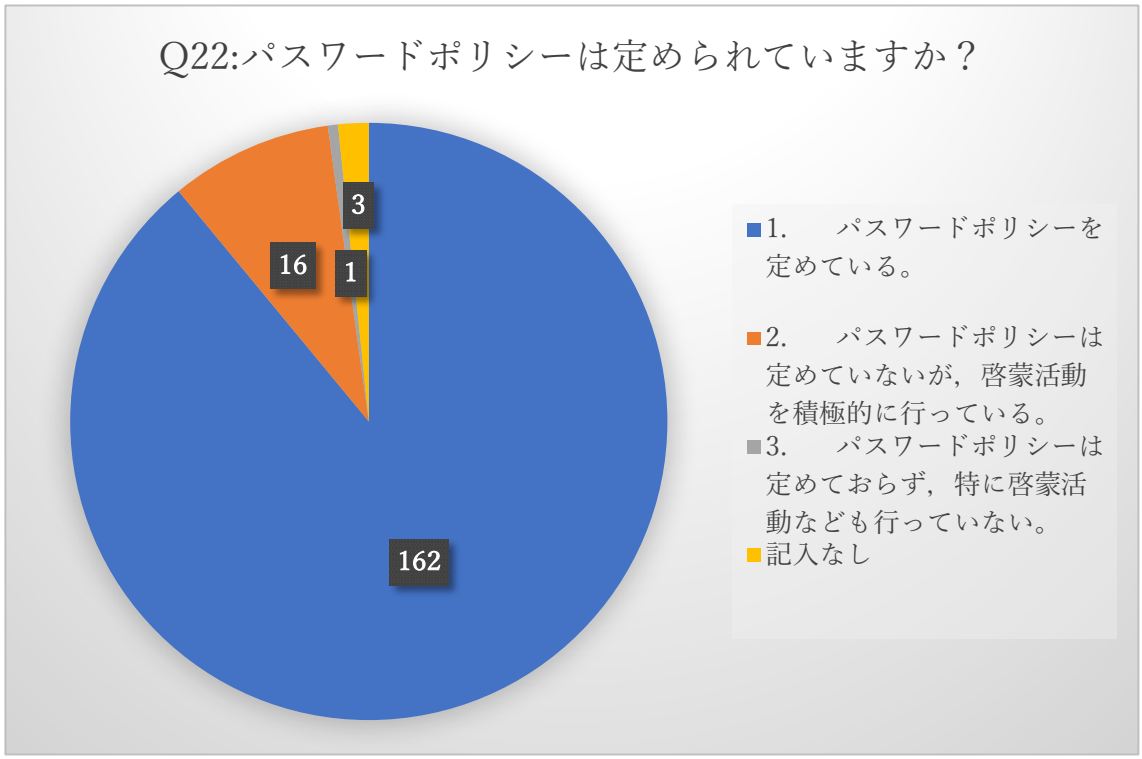
パスワードポリシー

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(Q1)。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。

共有 ID の禁止に関しても、各機関にて、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、自由記述の回答から読み取れました。

パスワードポリシーについても、ほぼ全ての機関において、パスワードポリシーがある、もしくは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)。





その他

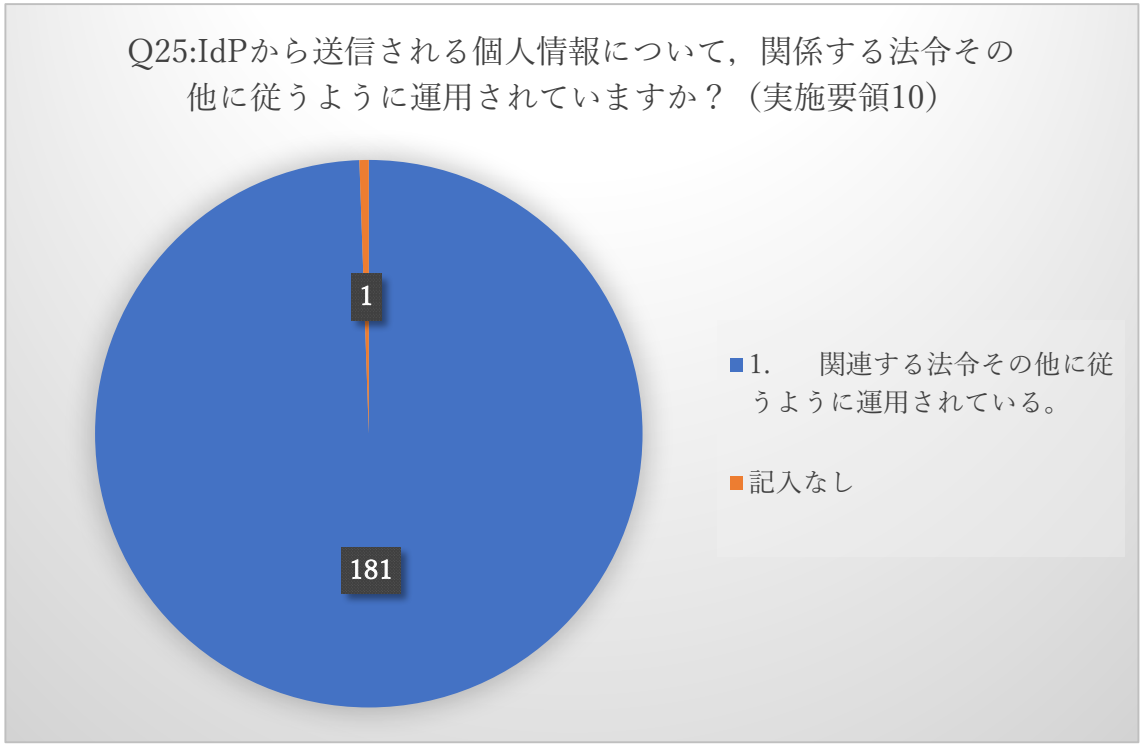
ログの保存期間については、多くの大学が 3 か月以上保存する運用となっています。前年度一部にみられた、学認技術運用基準にて推奨する 3 か月より短い保存期間を設定している機関はなくなりました。ただし、「定められていない」との回答がまだ一部みられます。最低保存期間を定めていただきたいと思います。

4　プライバシー（プライバシーに関係すること）

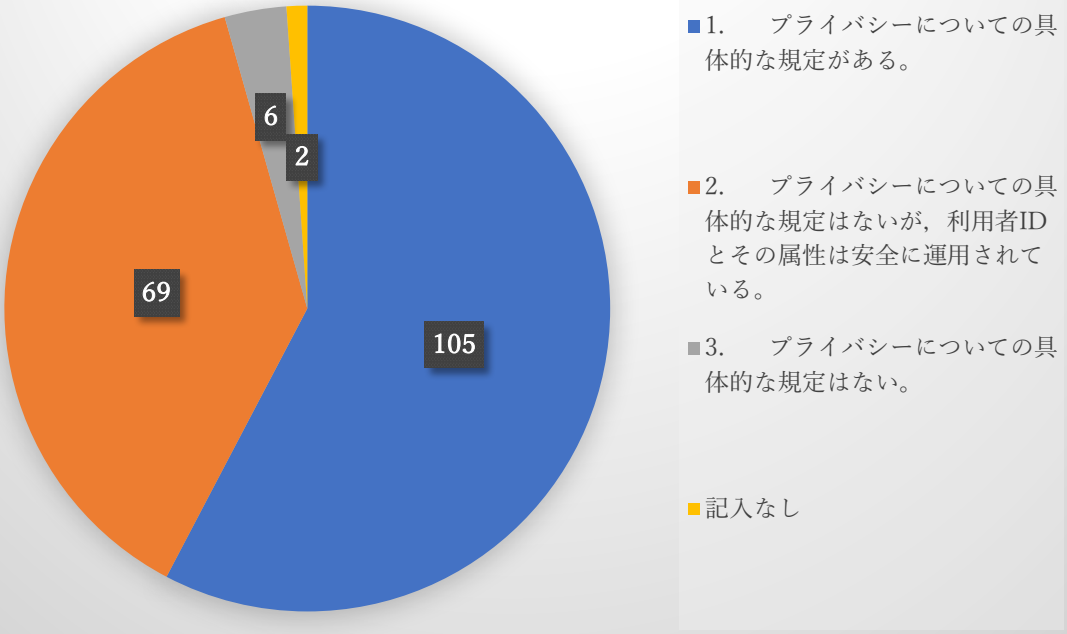
IdP から送信される個人情報については、1 件の未回答を除き、関係する法令に従うように運用されていいます(Q25)。未回答の 1 件は、「まだ全学での本格運用が始まっていないため、回答できない」との連絡を学認事務局が受けています。適法でない状態が放置されているということではありません。

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度同様 58%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 116 件（約 63%）（前年度は 59%）でした(Q27)。

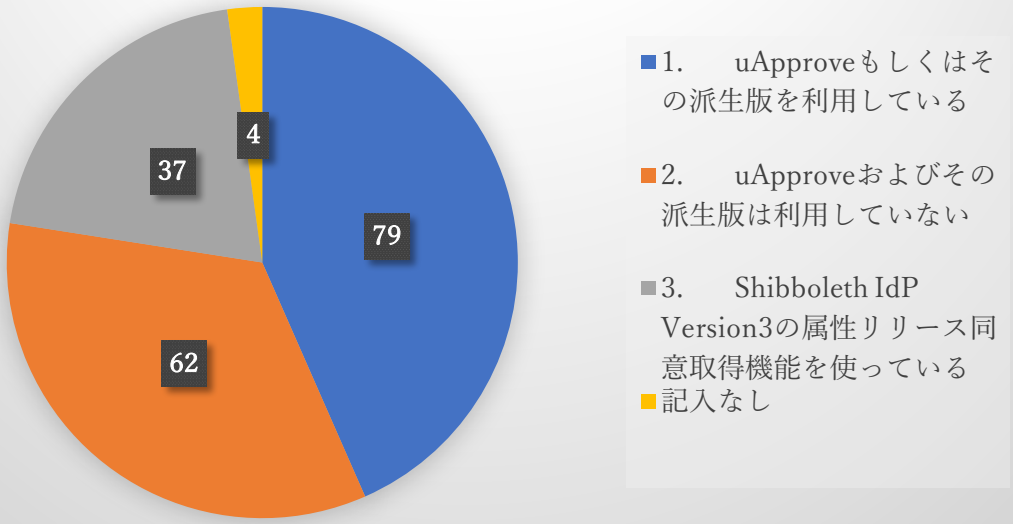
個人情報保護については、いずれも前年度とほぼ同水準を維持していました。



Q26:プライバシーについて，具体的に規定はありますか？



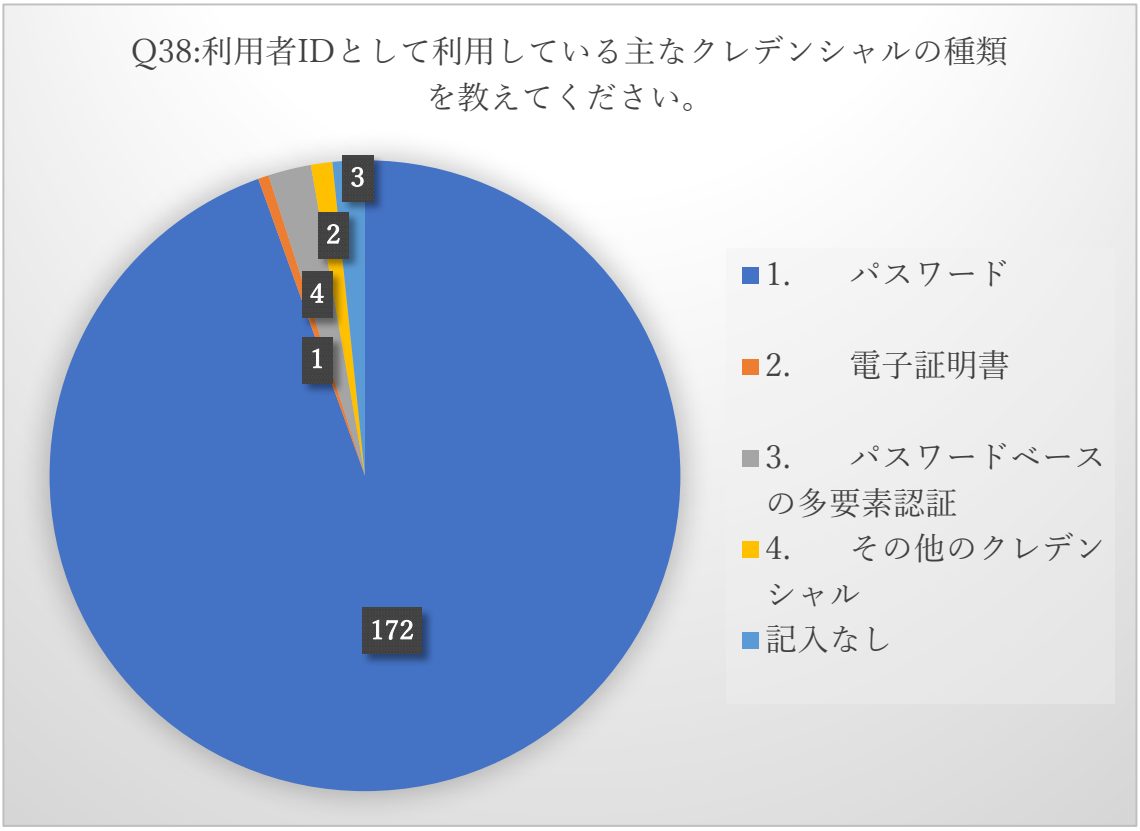
Q27:新たなSPのサービスを利用するとき，属性リリースの同意を得るためにuApproveもしくはその派生版を利用していますか？（技術運用基準8.6）



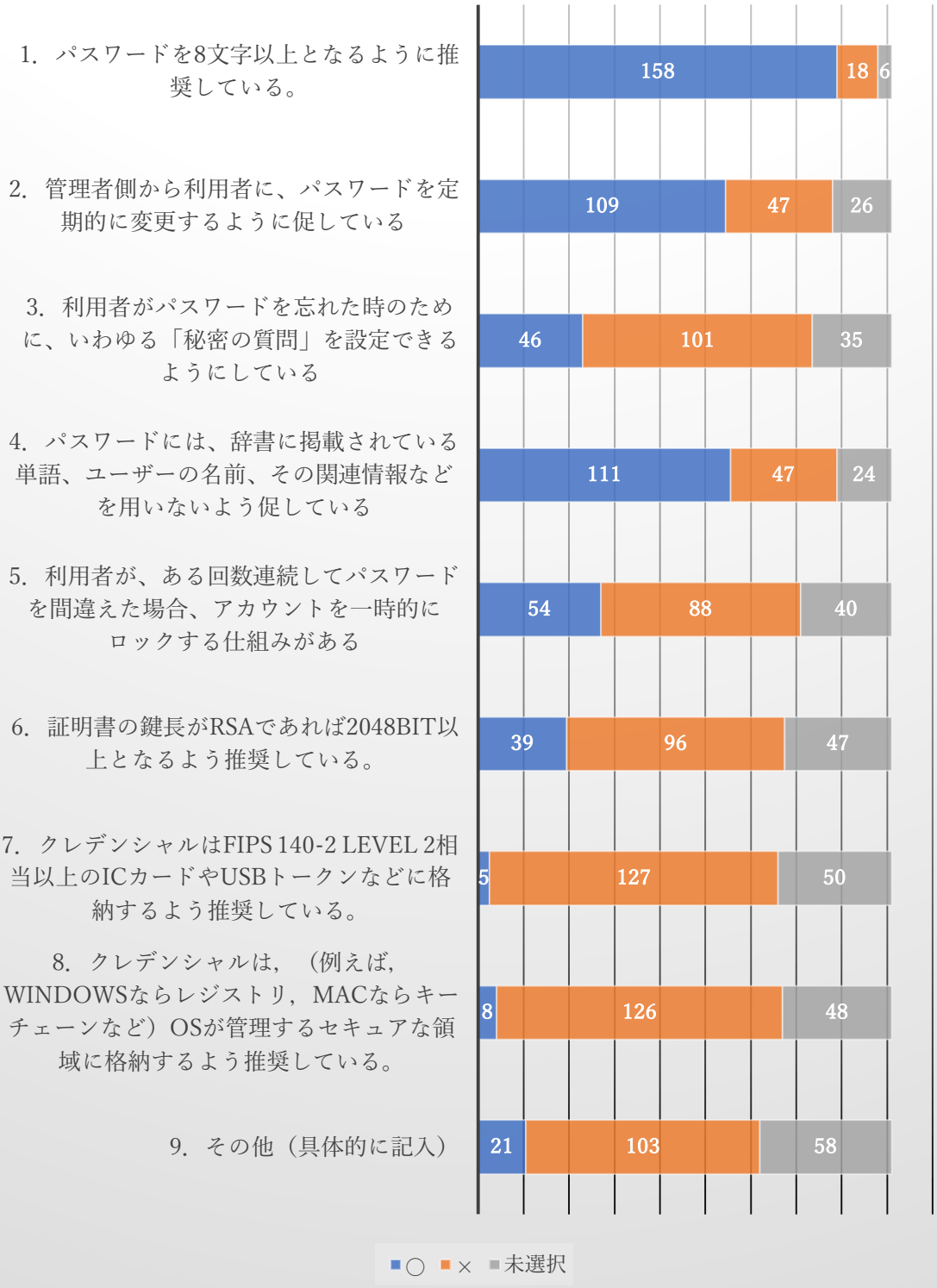
5　利用者 ID のクレデンシャル

前年度はこれ以降が任意回答の設問でしたが、今回の調査からは全問回答必須となりました。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、そのほとんどがパスワードであるとの回答でした。また、少数ながら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 カードによる認証を行っていると記述されていました。

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、2016 年に話題にあがった NIST-800-03 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ありません。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。



Q44:クレデンシャルの充分な安全性を実現する上で該当する取り組みがあれば教えてください。**（複数回答可）**



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。

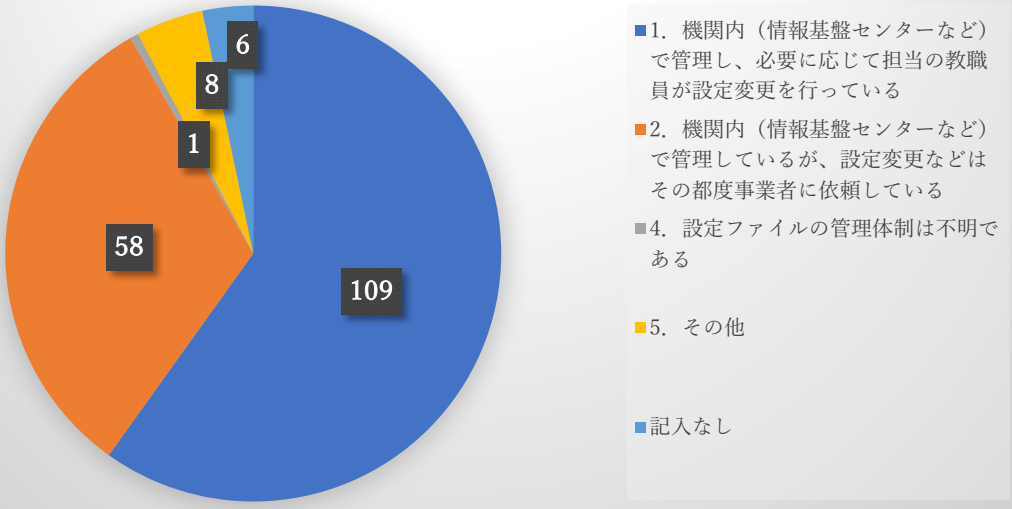
まず設定ファイルの管理（Q32）は、機関内での管理が 109 件（59%）、設定変更を都度外部に依頼しているとしたものが 58 件（31％）でした。IdP の設定ファイルは適切な管理（現状の最新版はどれで、現在 IdP に反映されているものはどれか？など）と設定変更が行えるようになっていれば問題はありません。管理体制が不明という回答が 1 件ありましたが、これは通常ありえることではありません。IdP の運用管理部局に確認するなどして、適切な取り扱いができるよう、管理体制を明確にしておく必要があるでしょう。

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。

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。86％の機関において、すでにアップグレード済みもしくは年度内にアップグレード予定であるとの回答であり、我々が想定していたよりも高い割合で移行が進んでいました。

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。アップグレード予定はないと回答した機関にも、この回答状況を鑑み、アップグレードを再検討いただきたいと思います。

Q32:IdPの設定ファイルの管理はどのように行われていますか？



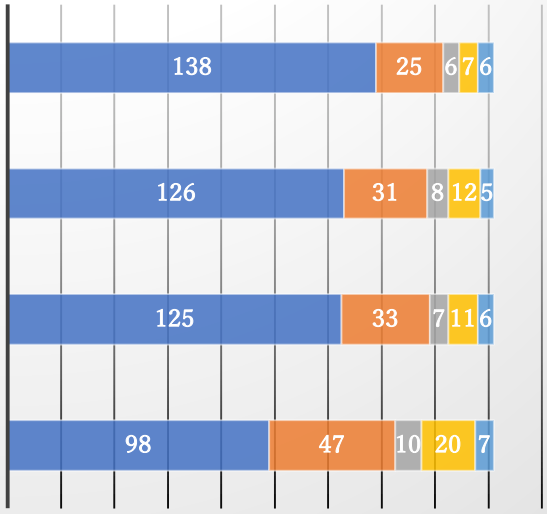
Q48:下記それぞれのメールにてお知らせした注意喚起への、本調査への回答時点での対応状況について教えてください。対象は2015年4月以降に事務局からお知らせしたものです。

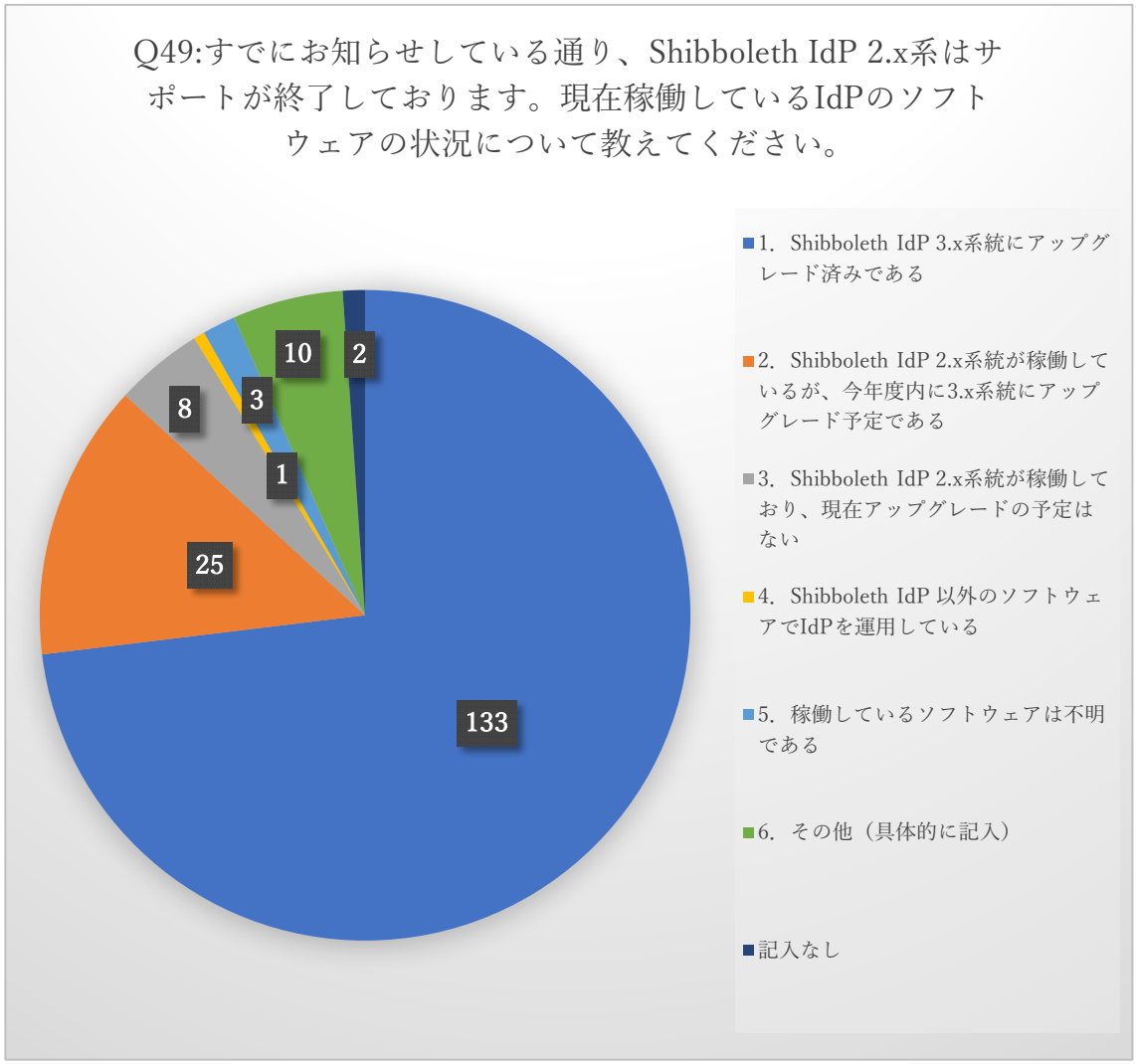
1. 件名：[IDP-CONTACT:00110]【注意喚起】OPENSSLの脆弱性について(2016/3/2)

2. 件名：[IDP-CONTACT:00111]【注意喚起】OPENJDKおよびORACLE JAVAの脆弱性について(2016/4/22)

3. 件名：[IDP-CONTACT:00112] OPENSSL脆弱性に関する注意喚起 (2016/5)

4. 件名：[IDP-CONTACT:00113]【注意喚起】CGIアプリケーション関連の脆弱性について(2016/7/19)




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。
133
25
8
1
3
10
2
1. Shibboleth IdP 3.x系統にアップグレード済みである
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
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
4. Shibboleth IdP 以外のソフトウェアでIdPを運用している
5. 稼働しているソフトウェアは不明である
6. その他（具体的に記入）
記入なし

以上