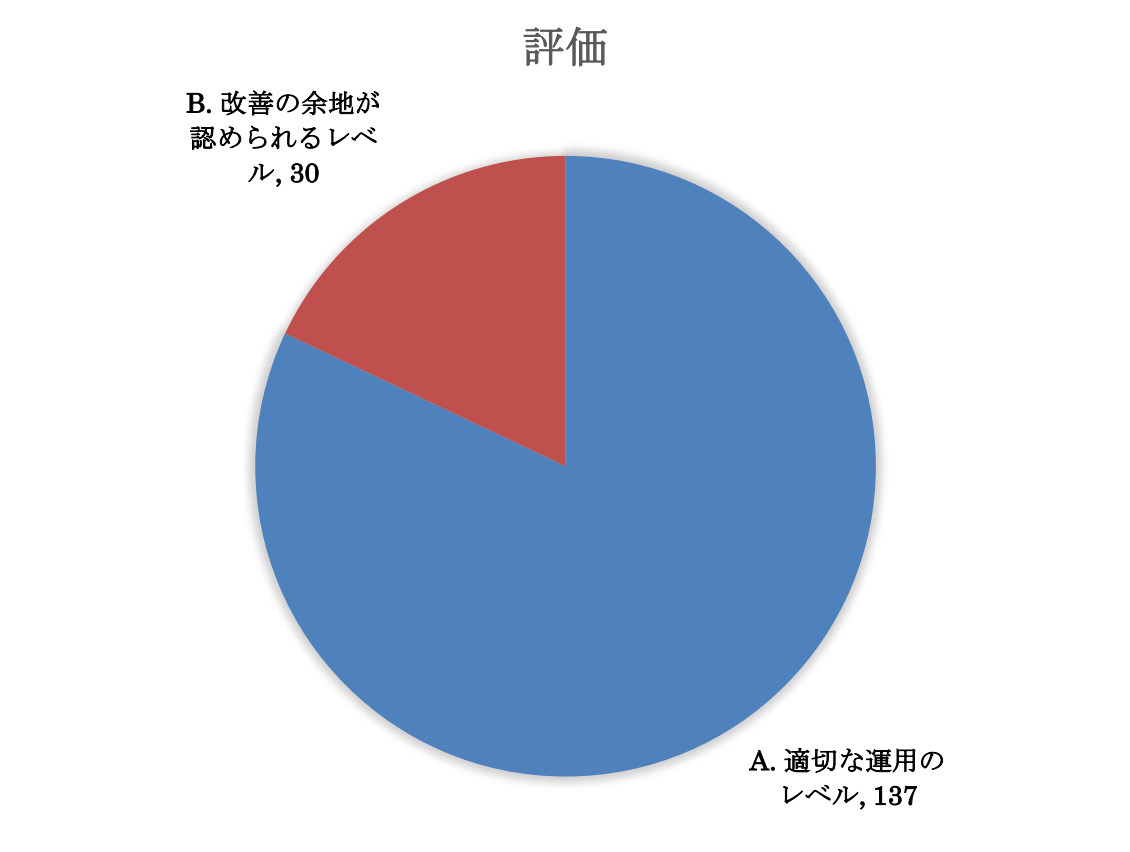
平成 28 年 1 月 20 日
トラスト作業部会

学認アンケート回答の精査報告

1. 総評

1.1. 評価結果

アンケート回答機関数は 167 件です。適切な運用を行っているのが 137 件であり、全体として良好な運用レベルです。一方、今回の評価基準で、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 30 件みられました。



本調査は、以下の 4 点を中心にすえて評価を行っています。

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アンケート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。

ここには、総評として、その中でもいくつか気になった点を述べておきます。

一つ目は、規則による統制（5.2.で詳述）についてです。IdP 運用上の根拠規則や内規の整備状況は、前年度より割合として増加しており、整備が進められていることがわかりました。IdP 運用上の規程類は、未整備であっても、ただちに B「改善の余地が認められるレベル」と評価されるわけではありません。他の要素での努力により、A「適切な運用のレベル」と評価された機関も多くあります。しかしながら IdP 運用上の規程類が制定されていない場合、運用担当者の裁量が大きいと見なすことが出来ます。運用担当者の裁量で現在運用できているにしても、継続的・安定的な運用のために、規則類の整備につとめて頂きたいと思います。

二つ目は、システム構成管理、とくに属性保証（5.3.で詳述）についてです。今回は 2 つの属性、o と eduPersonAffiriation に着目し、この 2 点が保証されているかをみました。9 割近くの機関で保証されていましたが、一部、保証していないと回答した機関もありました。両者を保証しないことが直ちに B 評価に結びつくものではありませんが、保証していない機関には、整備を進めて頂きたいと思います。

三つ目は、クレデンシャルの管理（5.5.で詳述）です。現状、ほとんどの機関で、利用しているクレデンシャルはパスワードでした。しかし、数としてはごく少数ながら、パスワードベースの多要素認証、電子証明書を用いた認証、FeliCa などの IC カードを用いた認証といった、気鋭の試みをしている意欲的な機関があることがわかりました。今後の拡充、増加に期待しています。

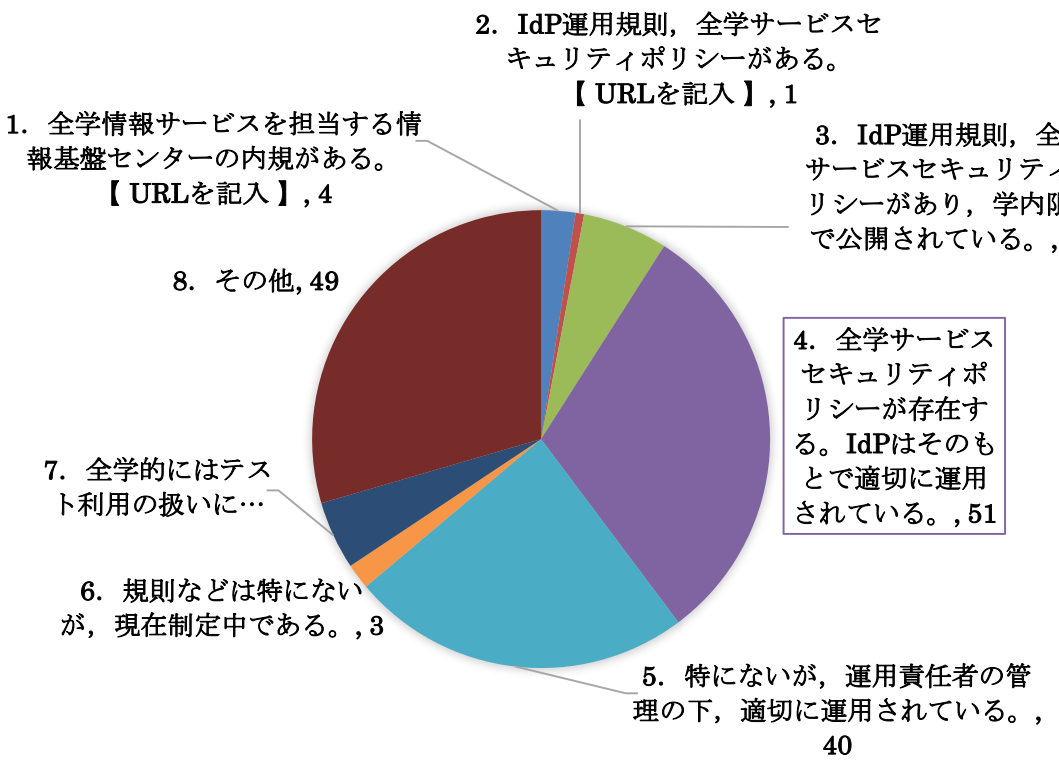
1.2. ガバナンス（規程の作成状況）

全学のセキュリティポリシーについては、151 件と 90%以上の大学で制定済みですが、定められていないとの回答が 14 件ありました(Q29)。なお、IdP 運用に関するセキュリティポリシーついては 70 件（42%）が定められているとの回答でした(Q30)。

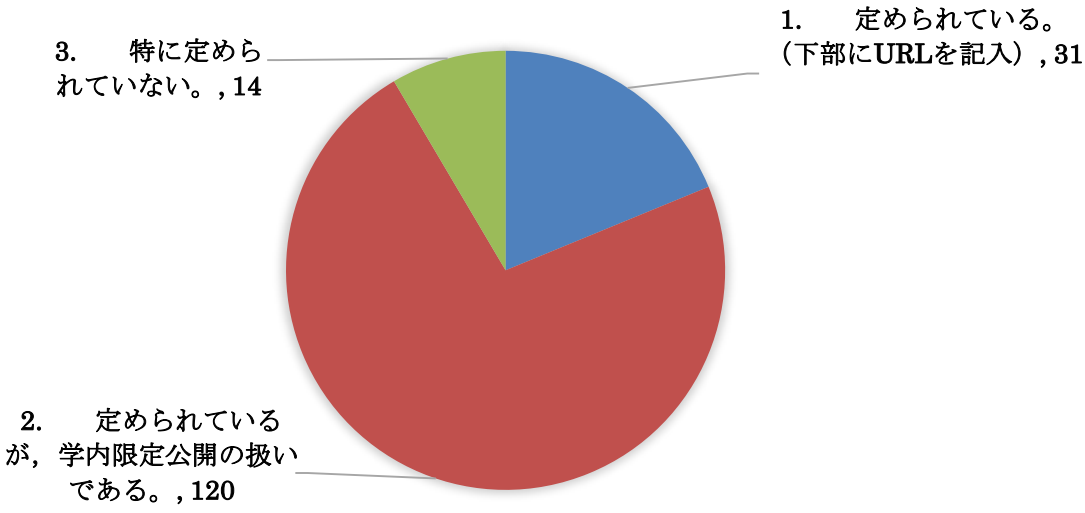
IdP 運用に関するなんらかの規則の制定状況については、セキュリティポリシーや運用責任者の管理のもと、適切に運用されている大学が多くみられます。IdPを対象として運用規則を制定している機関は前年調査では 47 件（前年度 136 件中、約 35%）でしたが、今回は 70 件（約 42%）となっています。前年度より規程の整備をお願いしてきましたが、各機関において順調にそれがすすめられていると考えます。従来からの参加機関にこの現状と必要性を丁寧に説明して、引き続き整備をお願いしていきたいと思います。

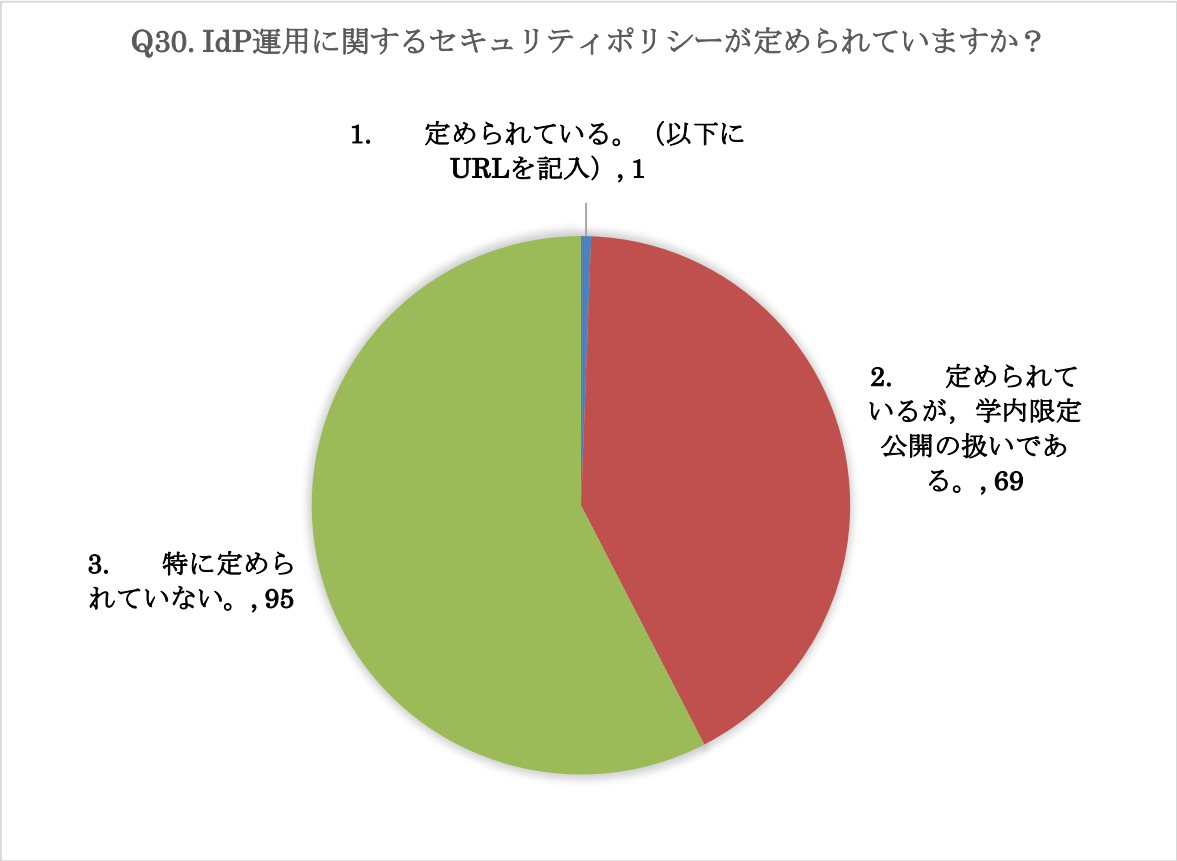
多くの機関において、利用者 ID の管理体制や全学的なセキュリティポリシーが整備されています。その基盤の上になりたって IdP が適切に運用されていることが読み取れます。Q8 において、なんらかの規程が整備されているとの回答は 66 件ですが、その他 49 件の自由記述の内容を読んでいくと、規程の整備状況をより丁寧に説明したものが多く見られました。前年度調査では IdP の運用規則やポリシーの策定率が低く、半数を切っていましたが、今回の調査では半数以上の機関で整備されていると読み取ることができます。

Q8. IdP運用上での根拠規則や内規の制定状況について



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，それにしたがって運用されていますか？





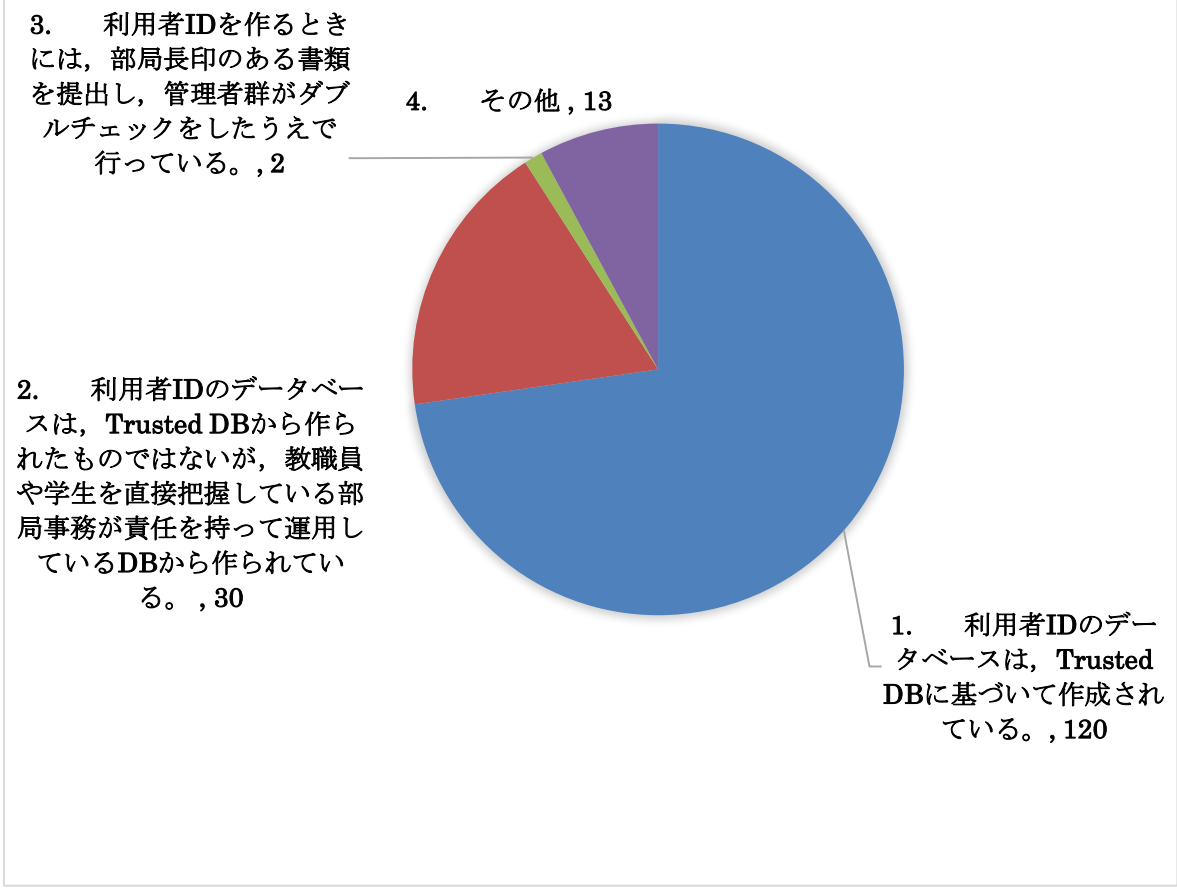
1.3. テクニカルなこと

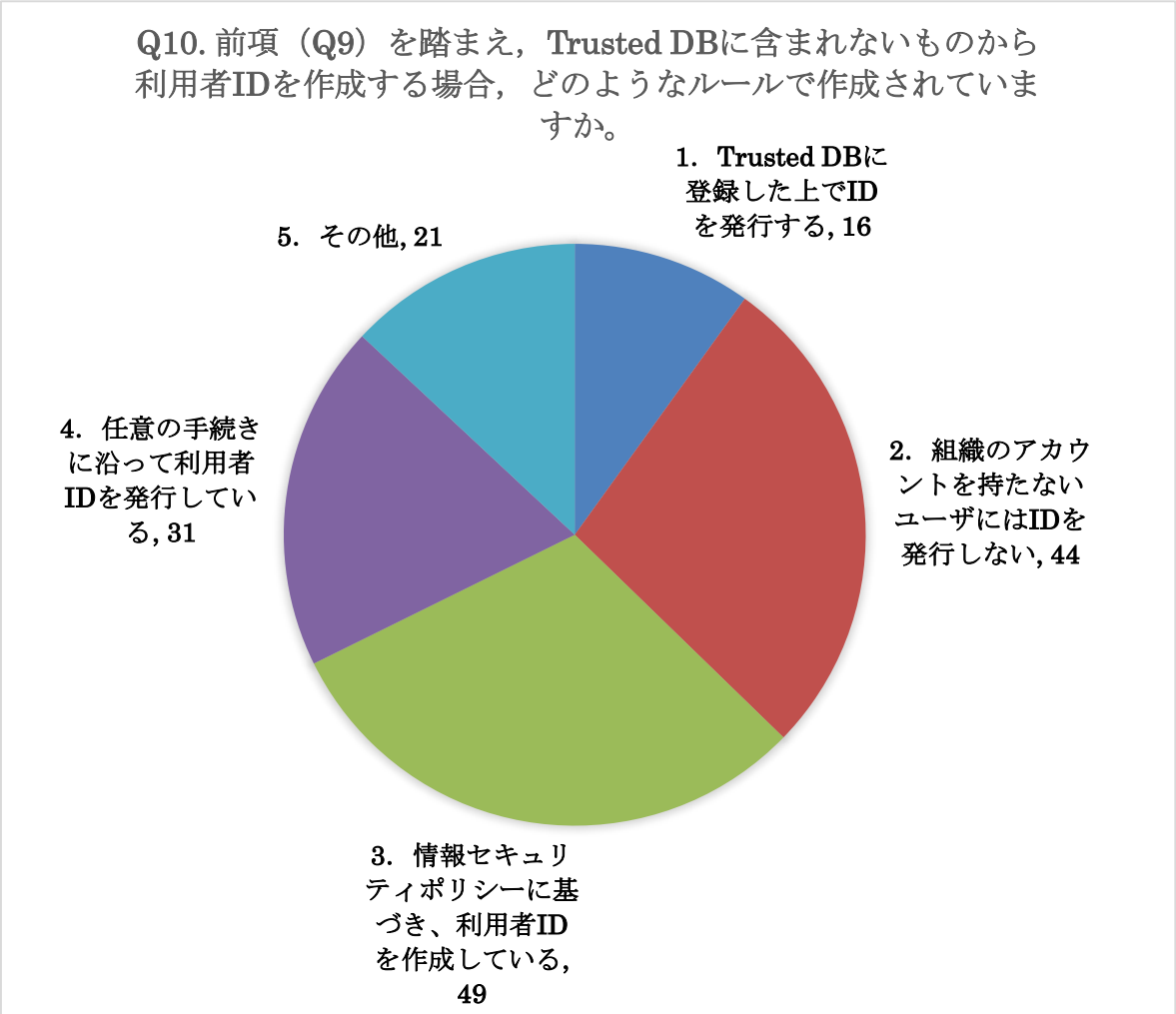
ID の運用状況（Trusted DB と直結しているかどうか）

前年同様、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ます(Q9)。しかし、Trusted DB に基づいて作成される以外の手法での 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、自由記述において、いくつかの機関において、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)。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？





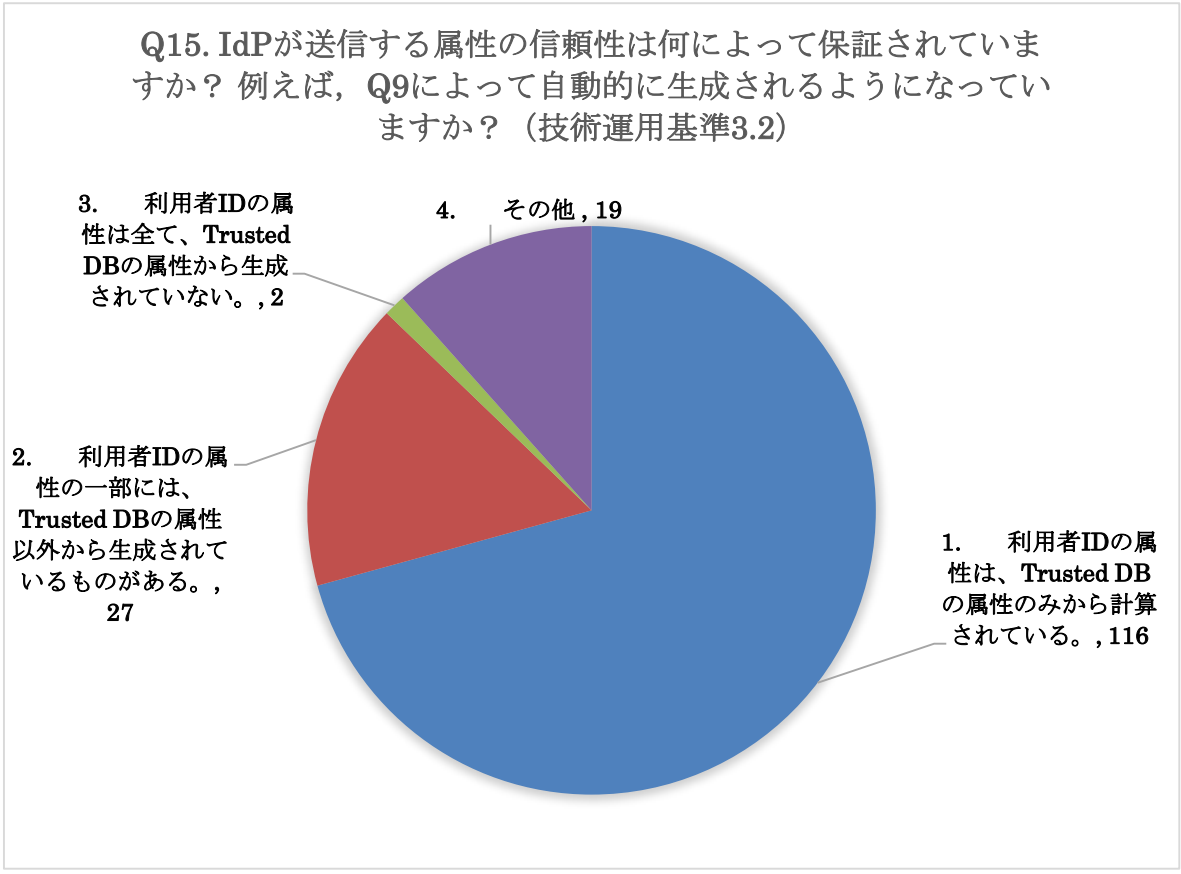
属性保証

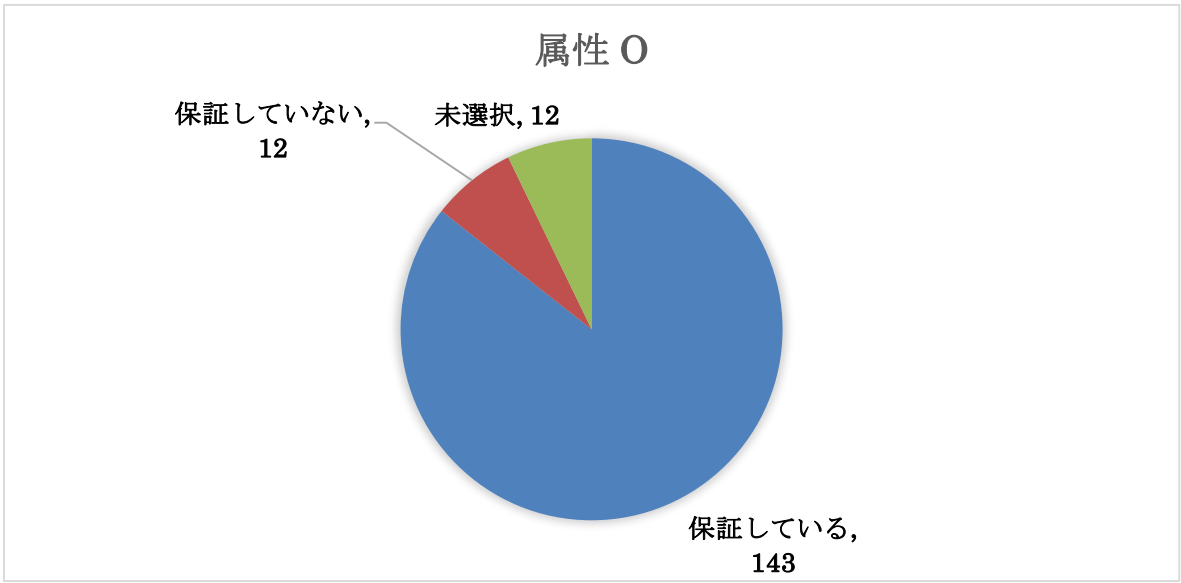
属性情報については、ほとんどの機関において、Trusted DB の属性のみから計算や、他組織の属性は付与しない体制となっており、システム運用基準 3.2 は正しく守られています(Q15)。

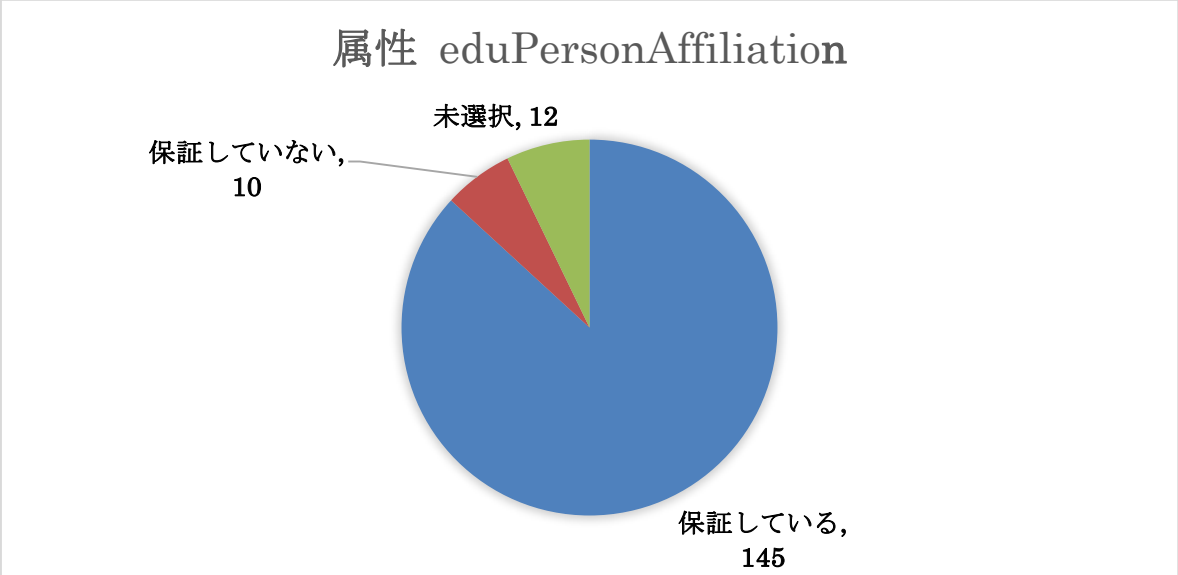
この設問には、「属性について，組織が保証しているものについて具体的にお答えください」といった問いが併せて設定されていましたが、前年度までは自由記述での回答となっていました。この自由記述の設問では無回答が多かったという反省をふまえ、今年度は学認で利用可能な全ての属性を列挙し、そのそれぞれについて「〇保証している」または「×保証していない」を選択できるようにしました。

今回はとくに 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「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れます。

今回の個別評価基準では、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。


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ますか？ 例えば，Q9によって自動的に生成されるようになっていますか？（技術運用基準3.2）
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
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。, 116


属性 O
保証していない, 12
未選択, 12
保証している, 143



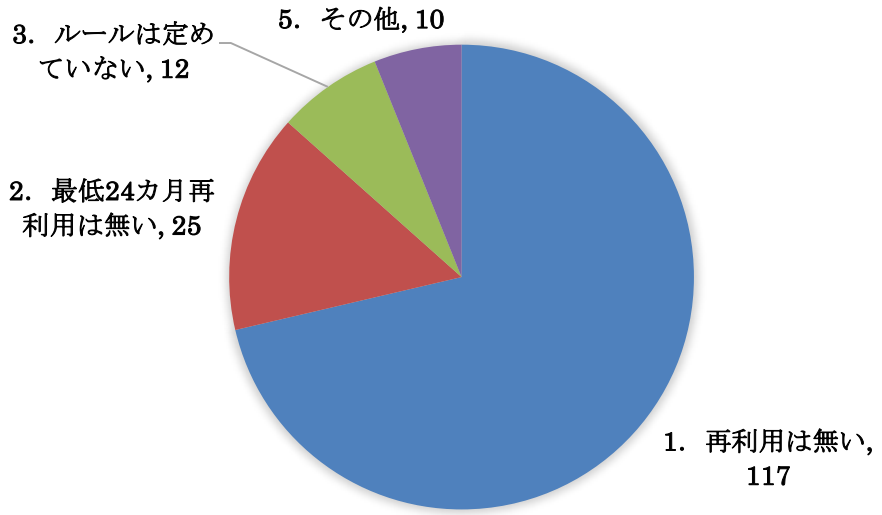
パスワードポリシー

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(Q18)。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。

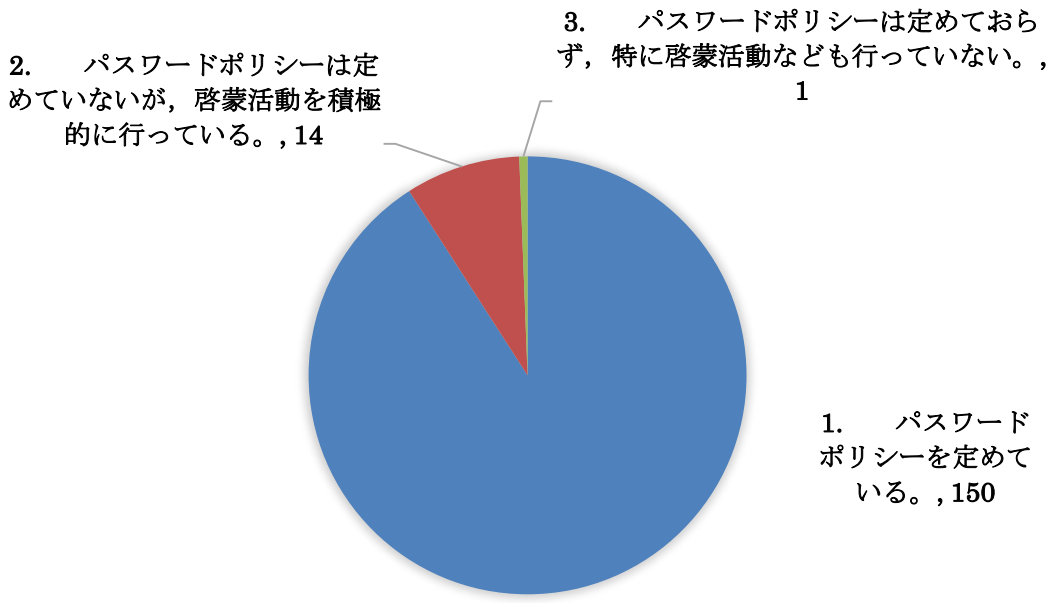
共有 ID の禁止に関しても、各機関にて、セキュリティ面からの啓蒙活動や、共有しなくても業務を行えるような運用が行われていることが、自由記述の回答から読み取れました。

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(Q21)。

Q18. 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）



Q21. パスワードポリシーは定められていますか？



その他

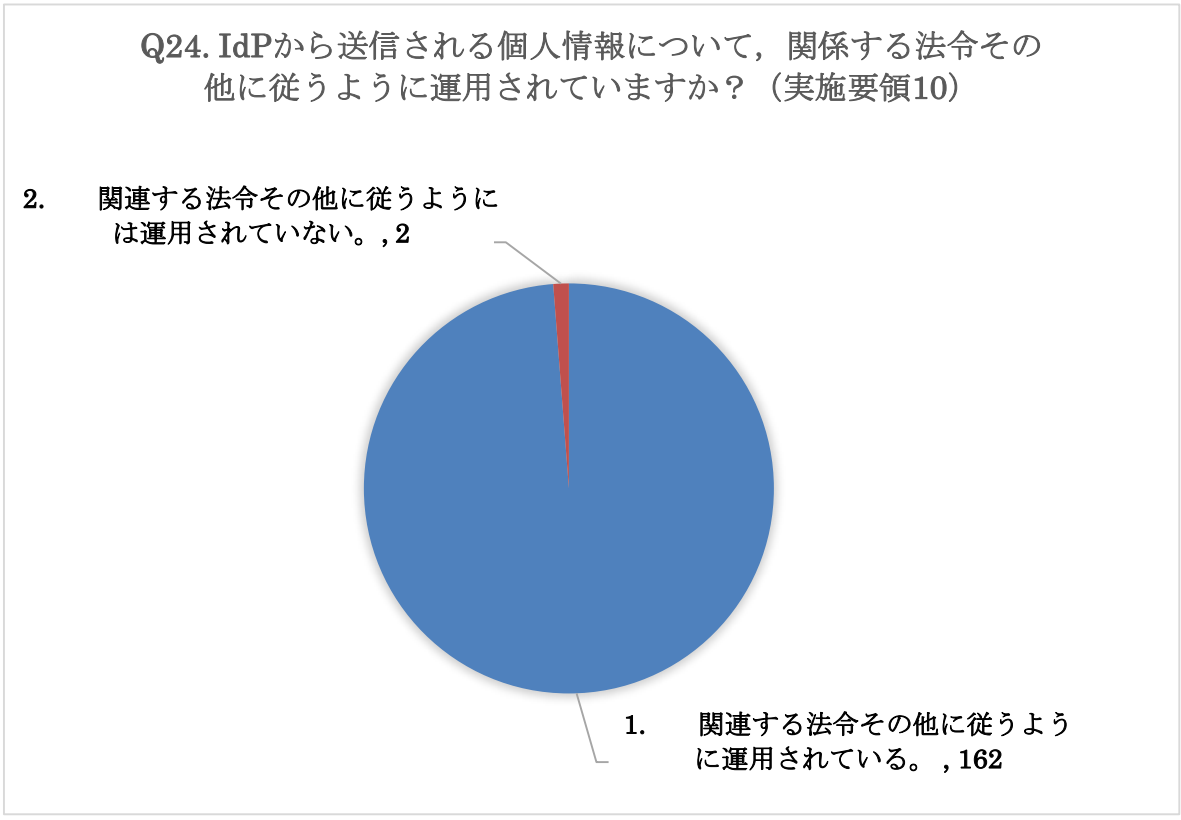
ログの保存期間については、多くの大学が 3 か月以上保存する運用となっています。しかし、一部にて学認技術運用基準にて推奨する 3 か月より短い機関が見られました。

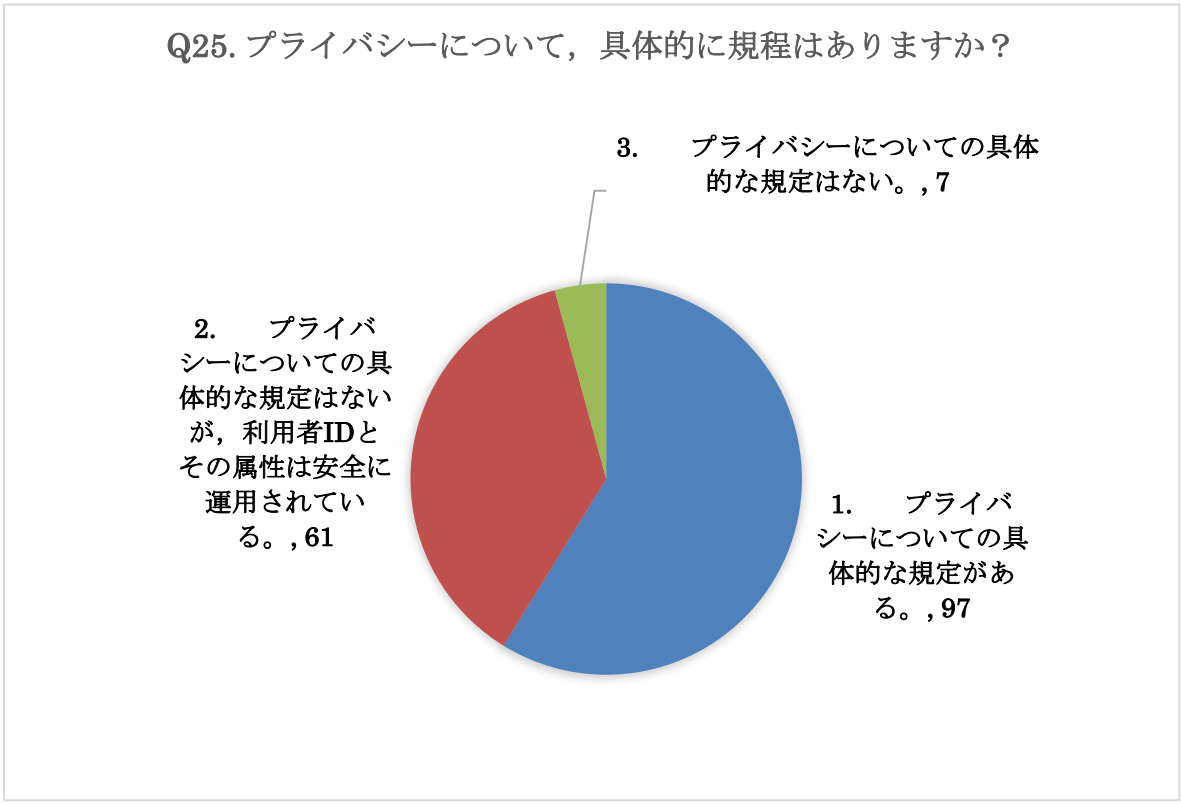
1.4. プライバシー（プライバシーに関係すること）

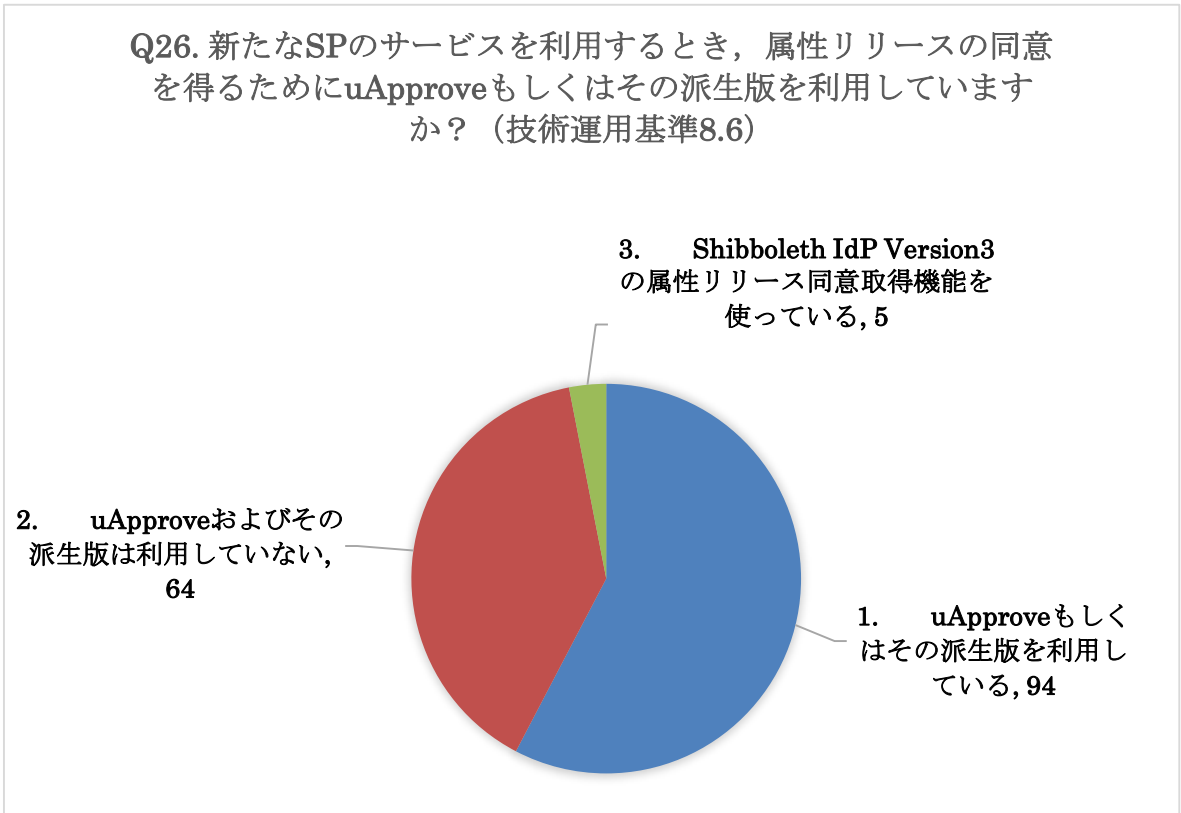
IdP から送信される個人情報について、関係する法令に従うように運用されていないと回答した機関が 2 件ありました(Q24)。関連する法令を理解したうえでそれに反する運用を行っていれば問題ですし、関連する法令が不明であればそれも問題です。不明なことがあれば、学認事務局までま照会するなどして明確にするようつとめてください。。

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同様 60%程度(Q25)、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 99 件（約 59%）（前年は 136 件中 70 件、51%）でした(Q26)。

個人情報保護については、規程の策定率は前年と同水準を維持し、属性リリース同意取得機能の導入率は前年より上昇していました。



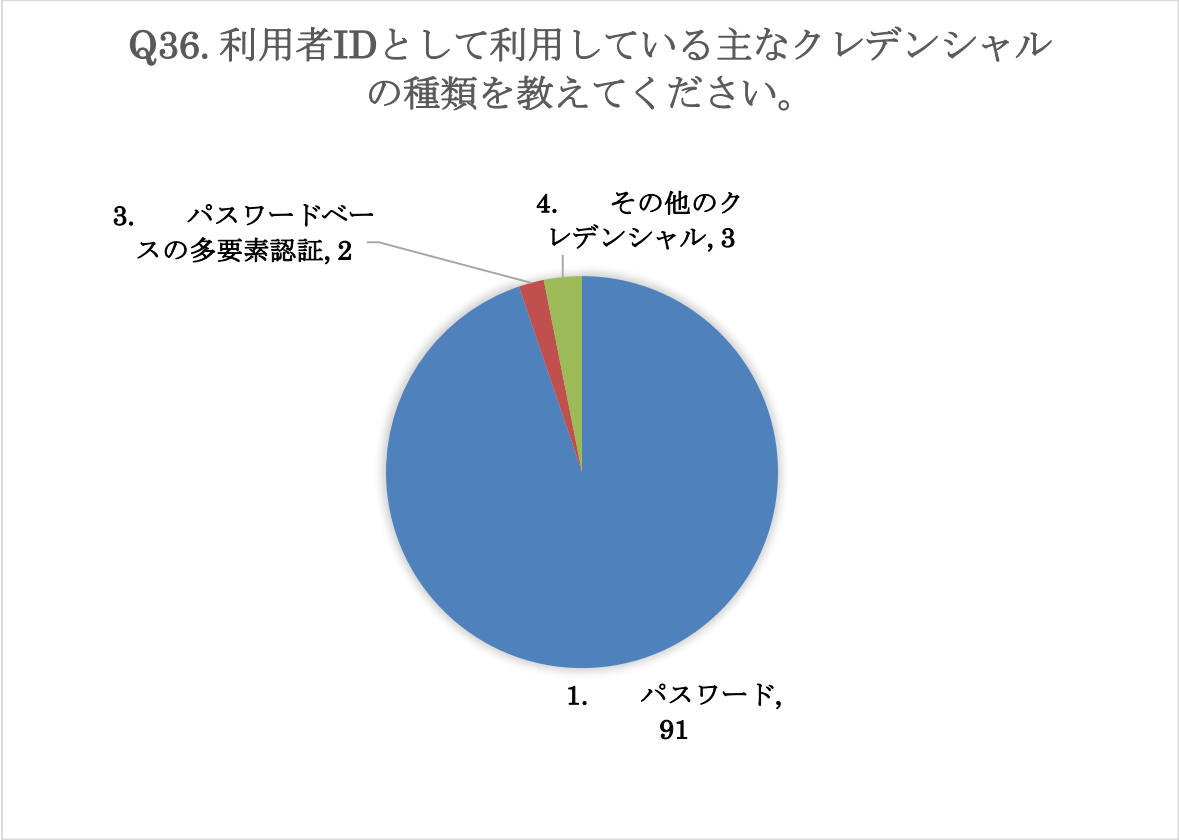




1.5. 利用者 ID のクレデンシャル

ここからは任意回答の設問になります。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

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。2 件でパスワードベースの多要素認証が導入されています。その他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。



以上