



学認参加IdP運用状況調査報告

佐藤周行
学認 トラスト作業部会主査



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、規程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
 - ▶ 2017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



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)」



- ▶ 未回答の組織がありました
 - ▶ 参加組織数199 回答組織数194
- ▶ 運用状況調査の意味
 - ▶ 一年に一回、運用チェックのために時間を割くことができる
 - ▶ 質問リストは、運用のチェックリストです
 - ▶ 自己評価の機会として積極的にお使いください
- ▶ 未回答が続くと、メタデータ送出の停止等を検討せざるを得なくなります
 - ▶ 是非とも避けたい
- ▶ 運用がつまらなくなったら
 - ▶ 知識を持っている人、尽力してくれる人が組織を去ってしまった等々
 - ▶ 一時的に運用停止をNIIに届け出るという選択肢があります
 - ▶ 運用に困難を感じたら、NIIに相談することもできます
 - ▶ 外出し...

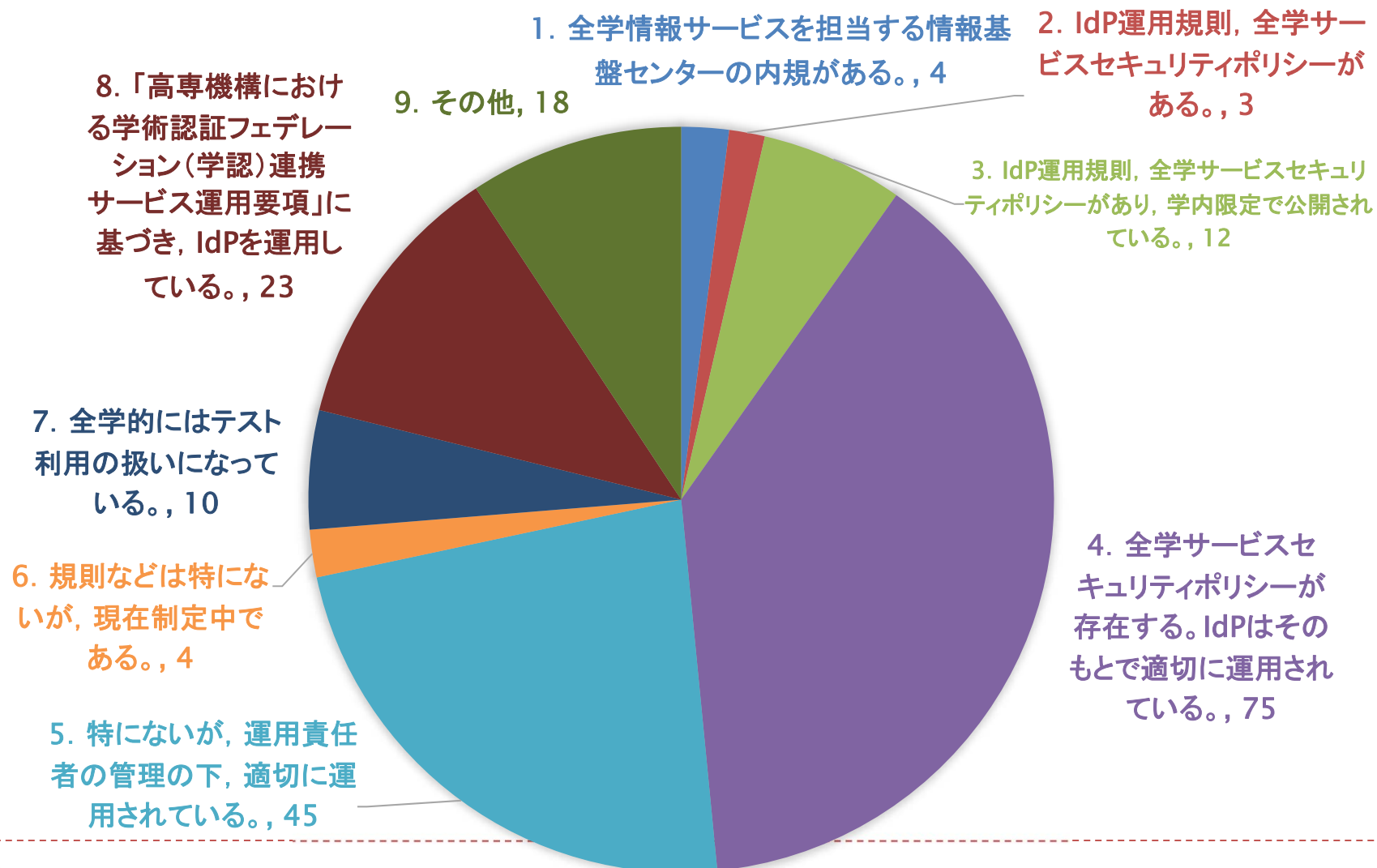


- ▶ 例年と同じレベルで運用が推移していることがうかがわれます
 - ▶ 継続してA評価をもらうところがほとんど。また、B評価も継続しがちである

- ▶ 以下、主だったものについて、評価の統計情報をお見せします。
- ▶ ガバナンス Q8
- ▶ テクニカル
 - ▶ アイデンティティ管理 Q9 Q18 Q33
 - ▶ クレデンシャル Q38 Q44
 - ▶ 構成管理 Q48



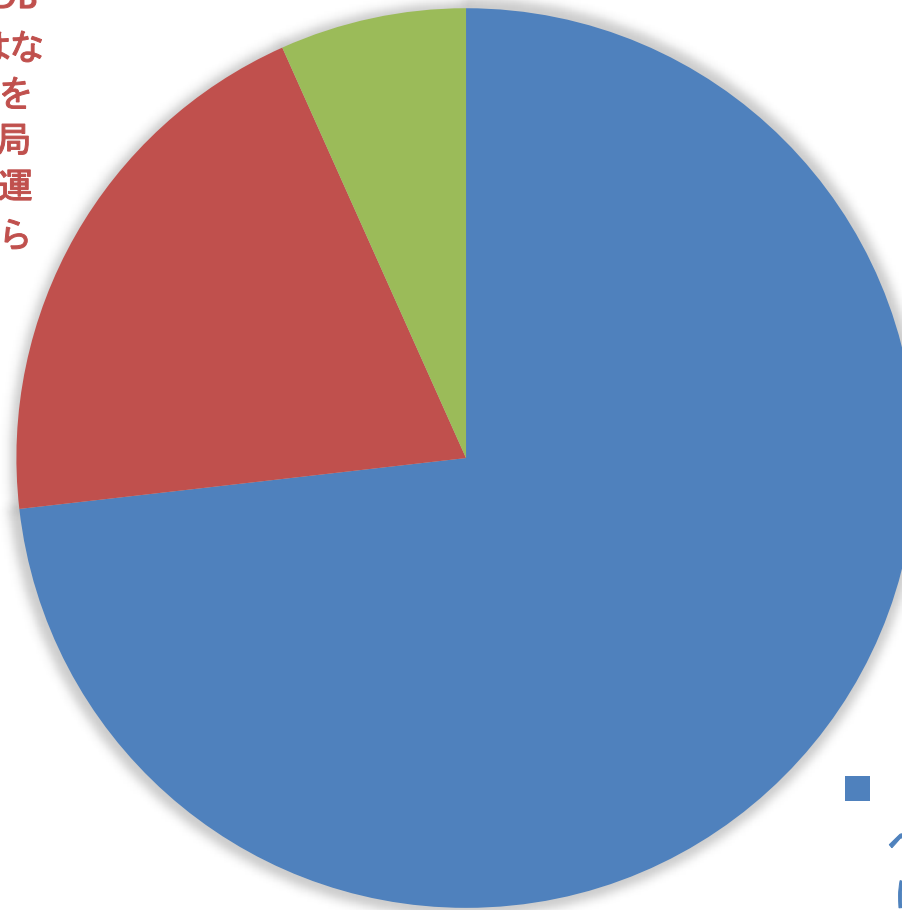
■Q8■ IdP運用上での根拠規則や内規の制定状況について



■Q9■ 利用者IDは、学務データや人事データ等、Trusted DBから作成されるように定めていますか？

■ 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。、39

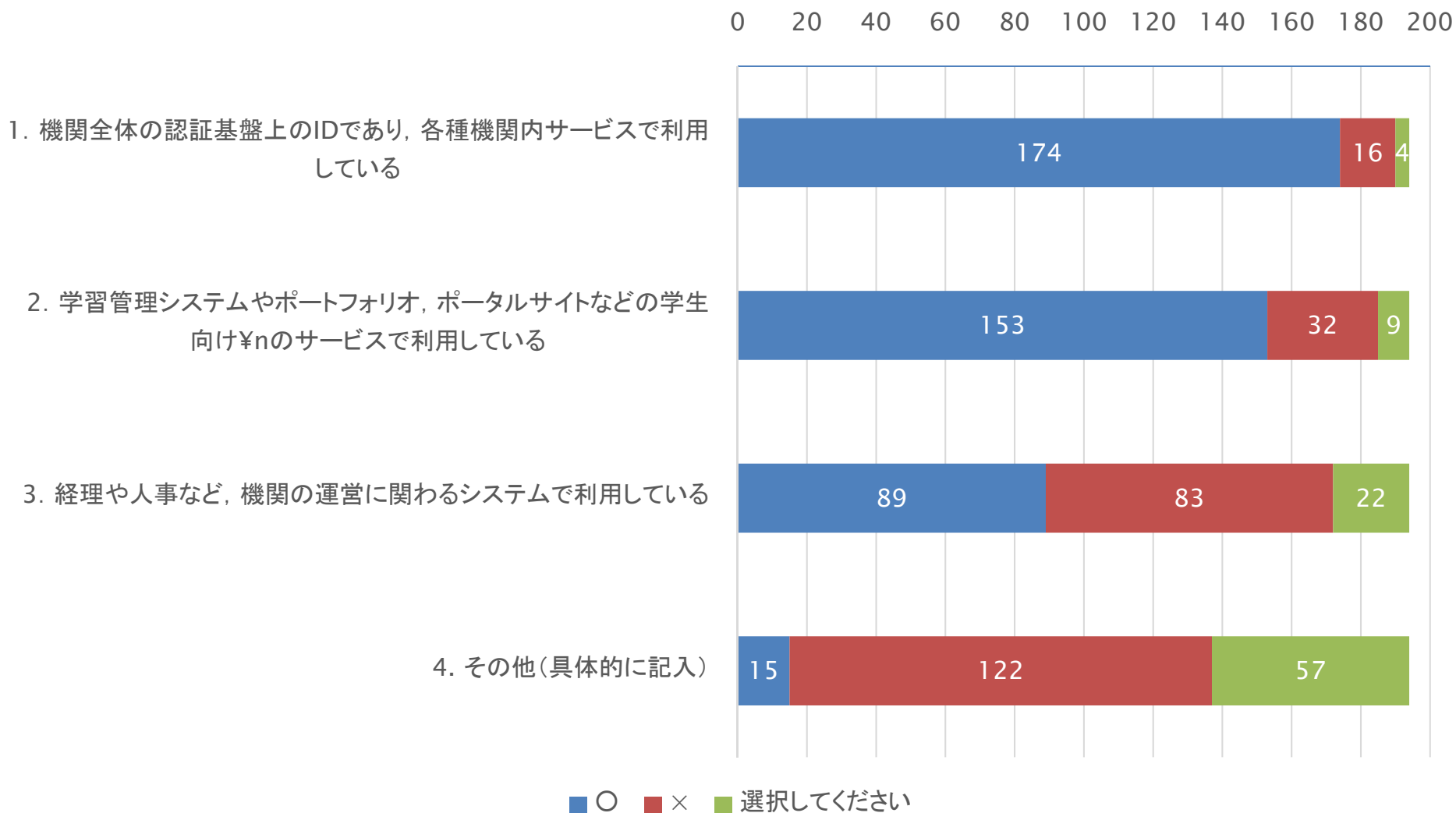
■ 4. その他, 13



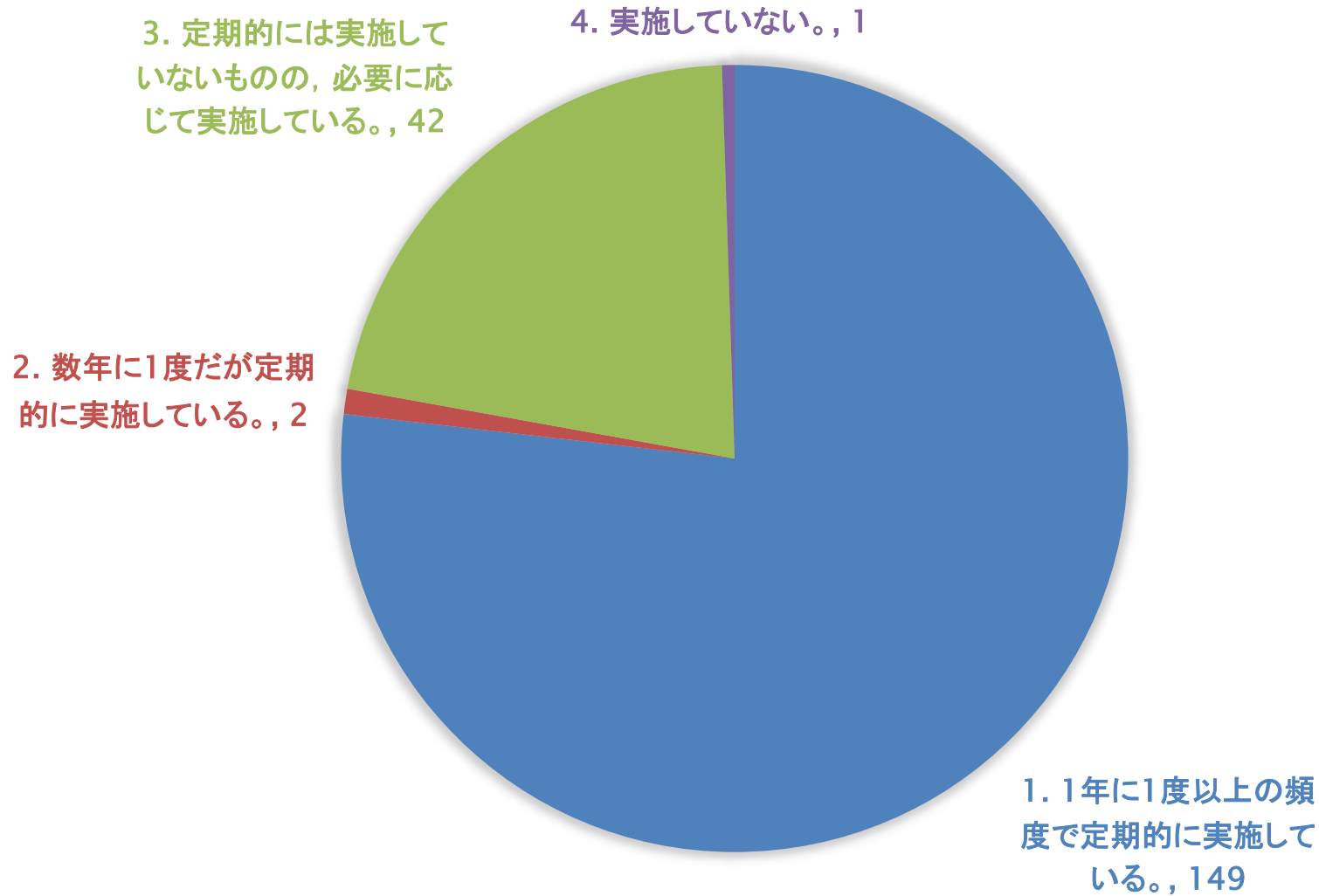
■ 1. 利用者IDのデータベースは、Trusted DBに基づいて作成されている。、142



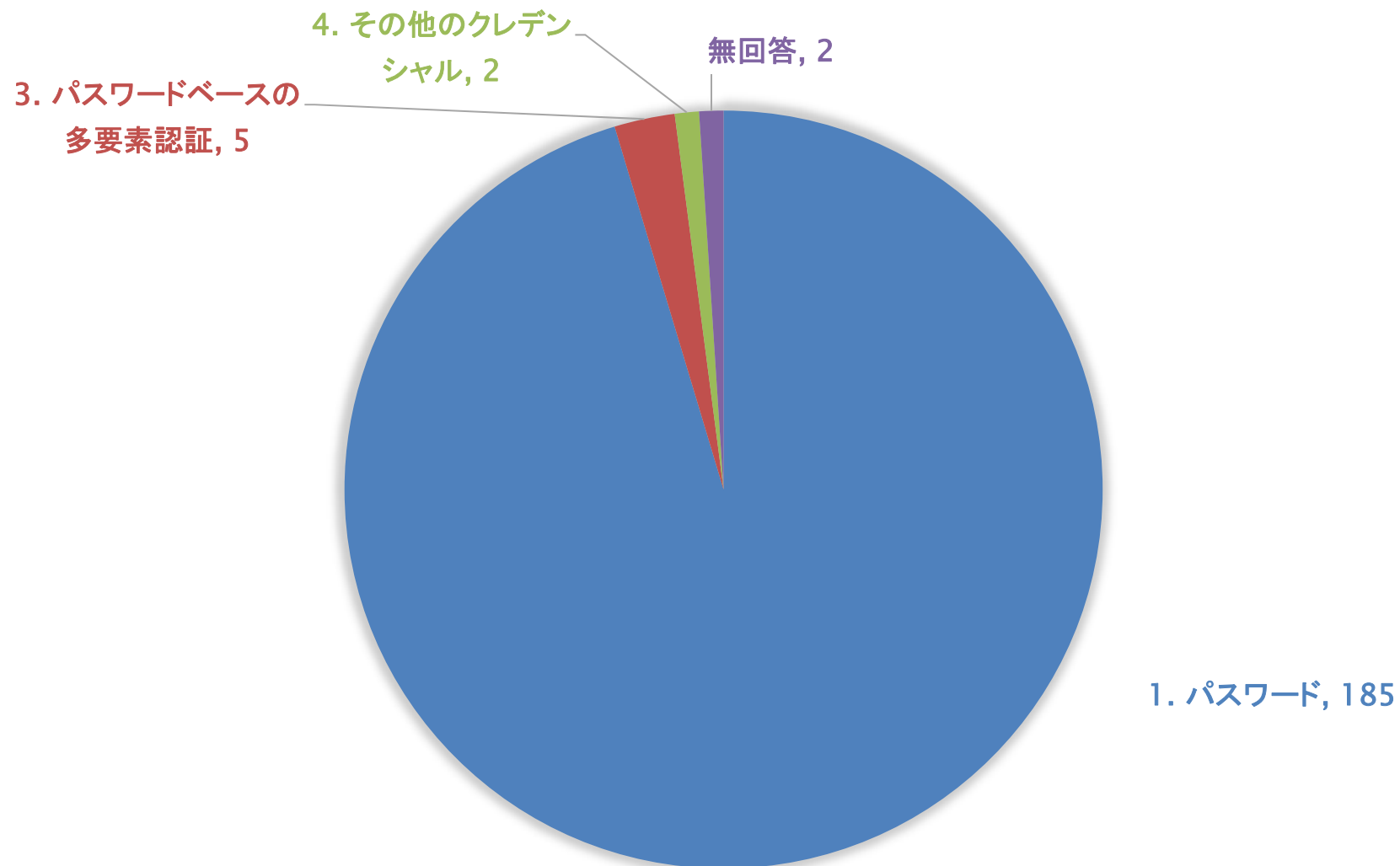
■Q18■ 利用者IDは, 学認以外に何に利用していますか？(複数回答可)



■Q33■ 利用者IDの定期的な停止・廃棄に関する手続きはどのようなタイミングで行うことにしていますか？

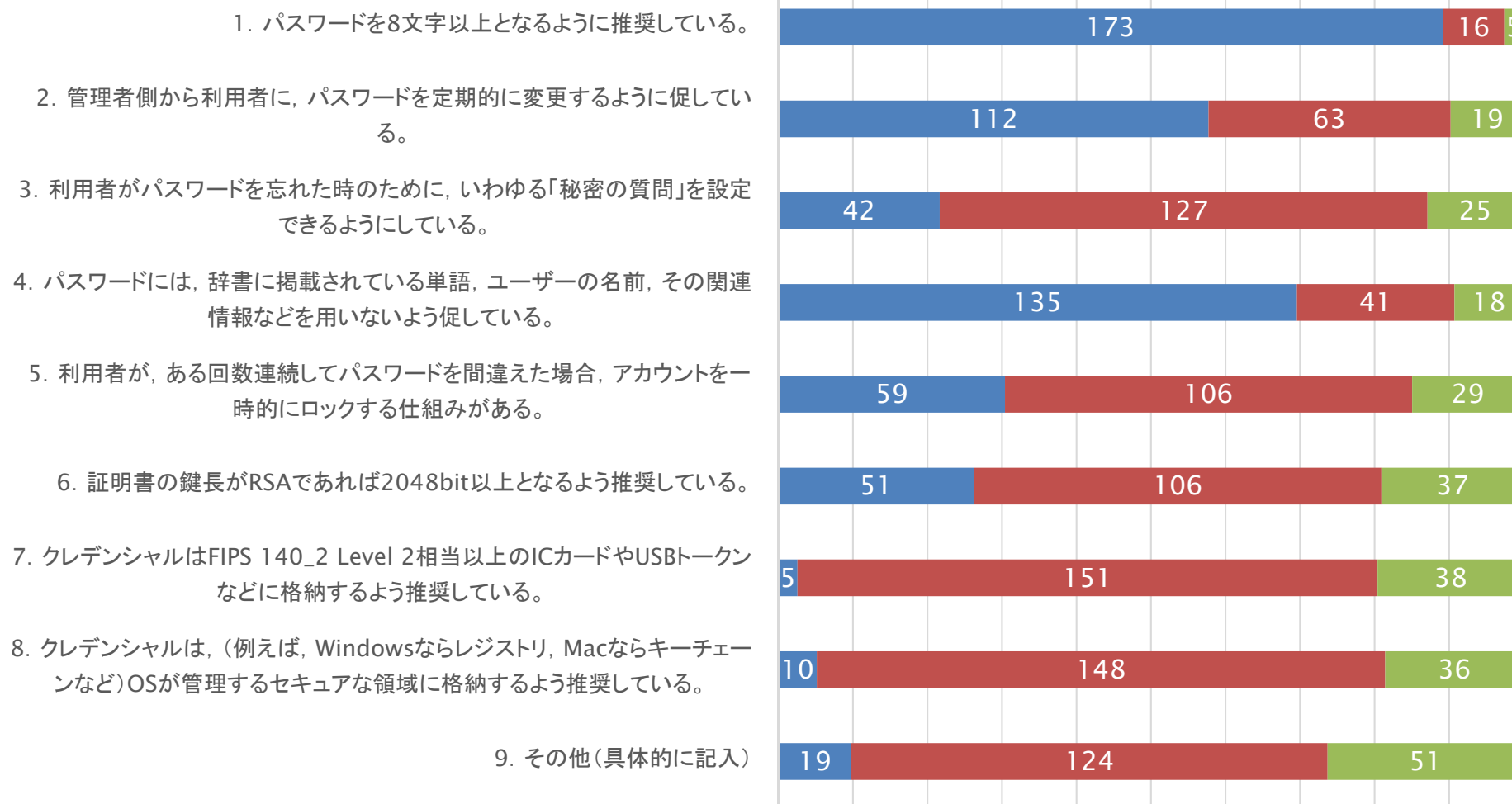


■Q38■ 利用者IDとして利用している主なクレデンシャルの種類を教えてください



■Q44■ クレデンシャルの十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)

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

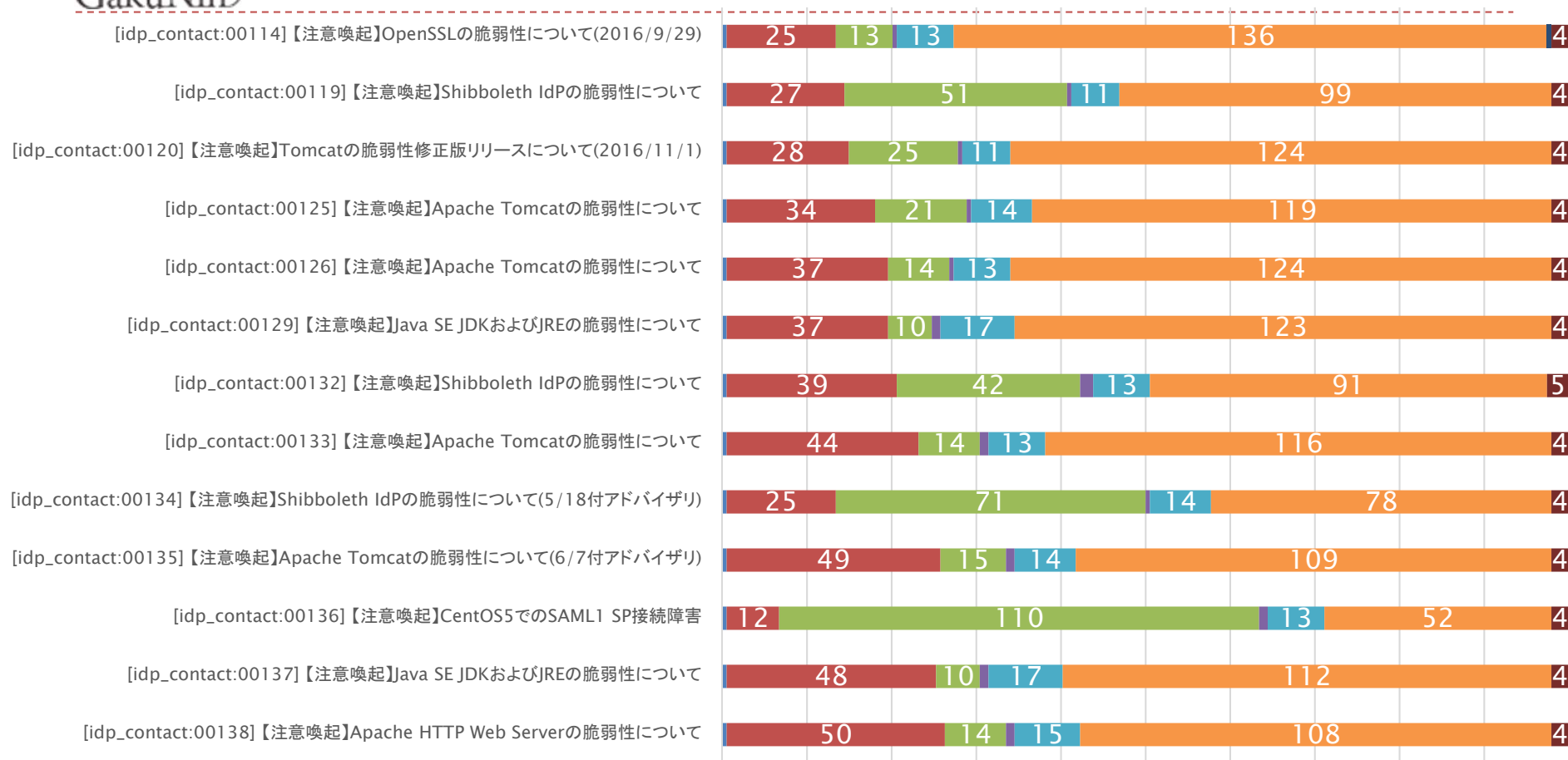


○ × 選択してください



GakuNin

■Q48■ 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。



対応予定はない

無回答

今年度中にアップデート予定である

対応状況が不明である

選択してください

対応不要だと判断した

当該ソフトウェアをアップデート済みである



パスワードの運用管理

- ▶ 今回は、パスワードポリシーについての質問をしました
 - ▶ 運用状況調査とは別扱いになっています
 - ▶ 調査結果は、統計処理をしたうえで報告

- ▶ 回答、どうもありがとうございました

- ▶ パスワードについては、議論が動いています
 - ▶ 米NIST SP800-63の改訂(2017)
 - JIPDECその他が対応用意
 - ▶ 総務省の規準の改訂等
 - ▶ パスワードより強い認証の導入

- ▶ 引続き、ご協力よろしくお願いします





GakuNin

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

