



学認参加IdP運用状況調査の講評

2017.6.7 学術情報基盤オープンフォーラム
国立情報学研究所 水元明法



調査の概要

- ▶ 本調査は、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に対するコンプライアンスの調査として、トラスト作業部会が実施した
- ▶ 2016年より、「**学認参加IdP運用状況調査**」と改名
 - ▶ 設問は学認アンケートを引き継いで作っている
 - ▶ 調査の連続性を確保している
- ▶ 調査対象
 - ▶ 2016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
 - ▶ Microsoft Excelで調査票を作成し、学認のWebサイトで公開した
 - ▶ 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た
- ▶ 回答期間
 - ▶ 2016年9月30日から11月1日まで
- ▶ 回答数
 - ▶ 182機関 (100%)



評価基準(2015)

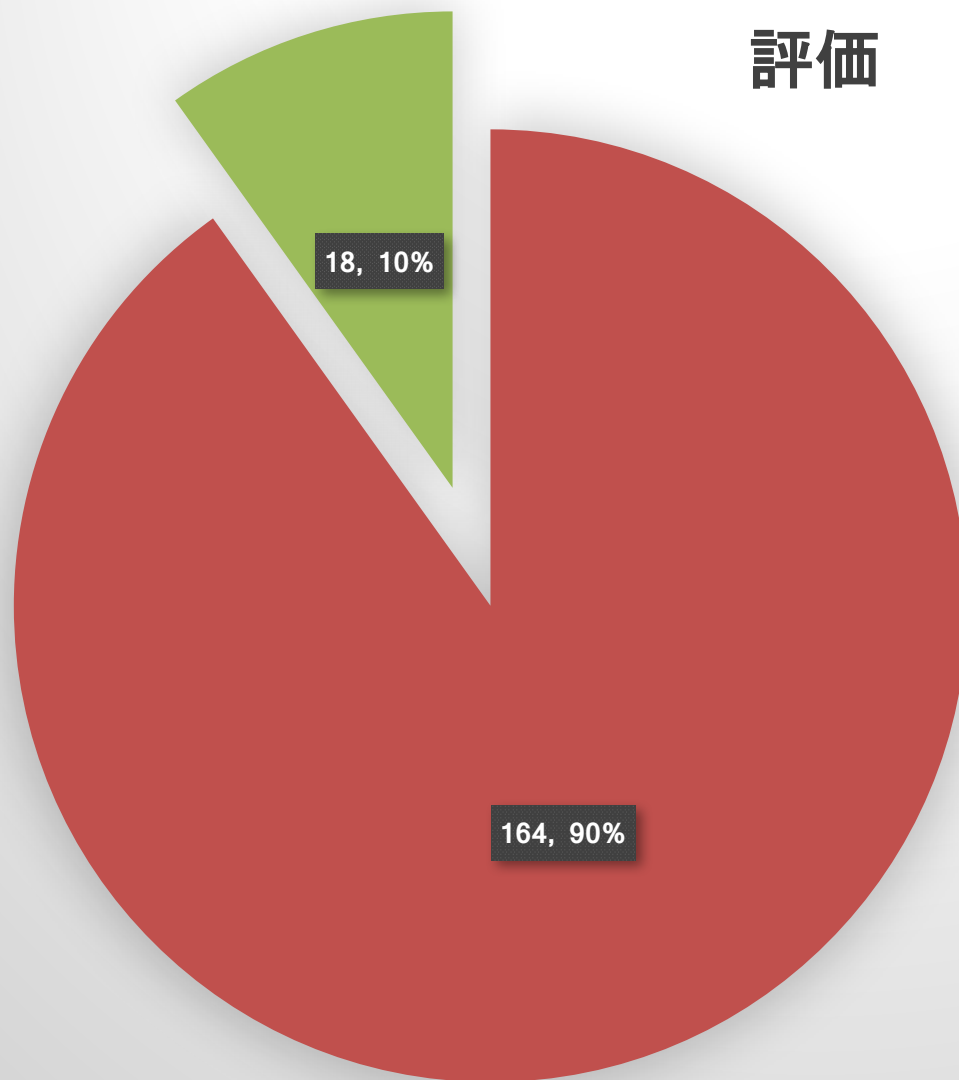
- ▶ IdP運用上、配慮すべき点として下記の4つがあげられる
 - ▶ 運用の統制(Control)。特に規則による統制
 - ▶ 運用アイデンティティの運用管理(アカウントのライフサイクル管理)
 - ▶ システムの構成管理(configの適切な管理)
 - ▶ パスワード(クレデンシャル)の管理
- ▶ 2015年度の評価基準は、これら4点をもとに下記の通り設定した
 - ▶ IdPを運用する上での根拠規則や内規の制定状況
 - ▶ 利用者IDと属性の管理・運用について
 - ▶ 利用者IDはTrusted DBから作成されているか
 - ▶ 保証している属性について。とくに以下の2属性
 - o(組織名)
 - eduPersonAffiliation
 - ▶ 個人情報保護について
 - ▶ とくにuApproveまたはその派生版、IdP V3の同等機能を使用しているか
 - ▶ 利用者IDのクレデンシャルについて



評価基準(2016)

- ▶ 2015年基準に加えて....
- ▶ 2016年調査では下記の基準を追加した
 - ▶ 設定ファイルの管理体制について
 - ▶ 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
 - ▶ Shibboleth IdP version 2系統がEOLを迎えたことによる、version 3系統へのアップグレード状況
- ▶ この基準に従って、組織全体として運用のレベルが保たれているかどうかについて個別に回答を精査した
- ▶ 評価は下記の2段階で行った
 - ▶ 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)

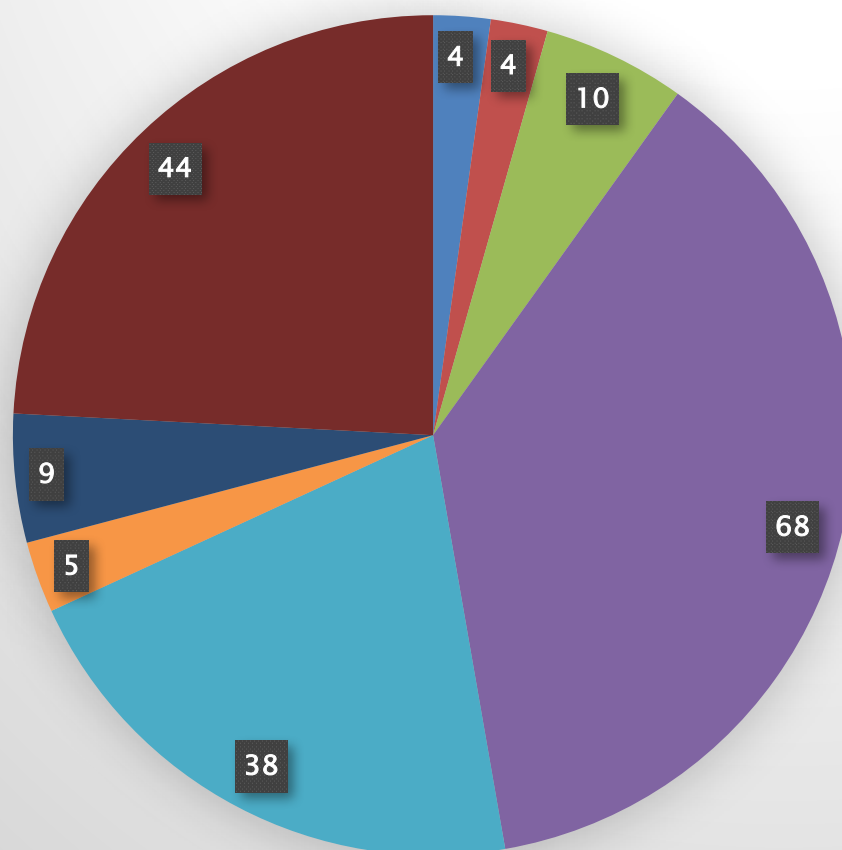
評価



- 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)

ガバナンス — 規程の策定状況

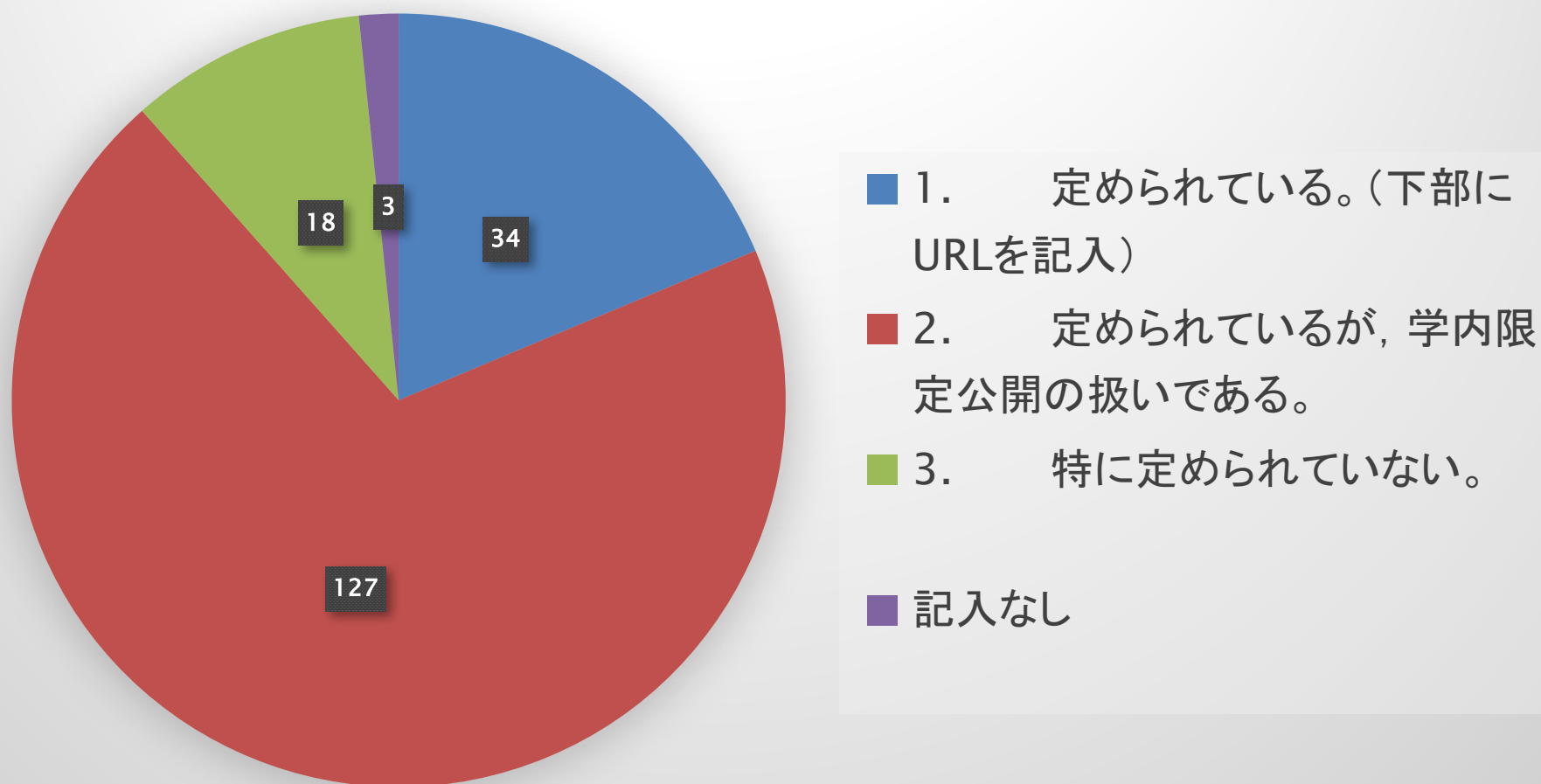
Q8:IdP運用上での根拠規則や内規の制定状況について



- 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

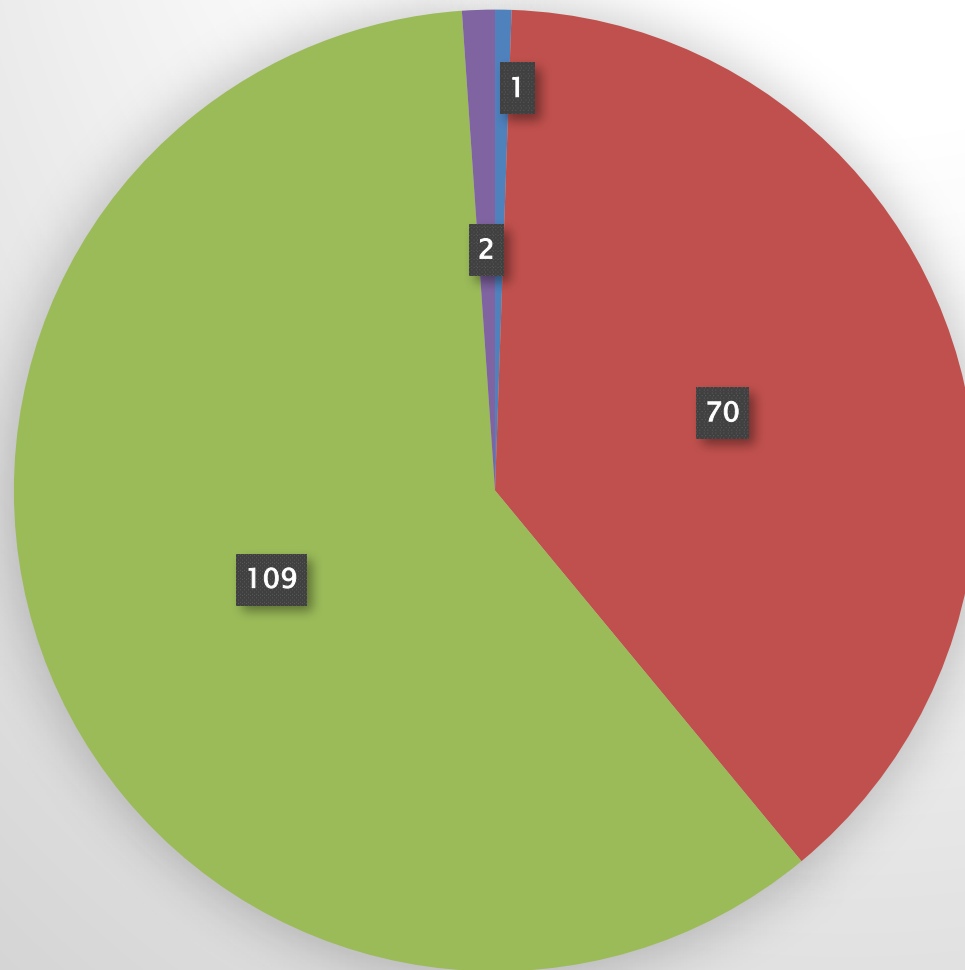
ガバナンス — 規程の策定状況

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？



ガバナンス —規定の策定状況

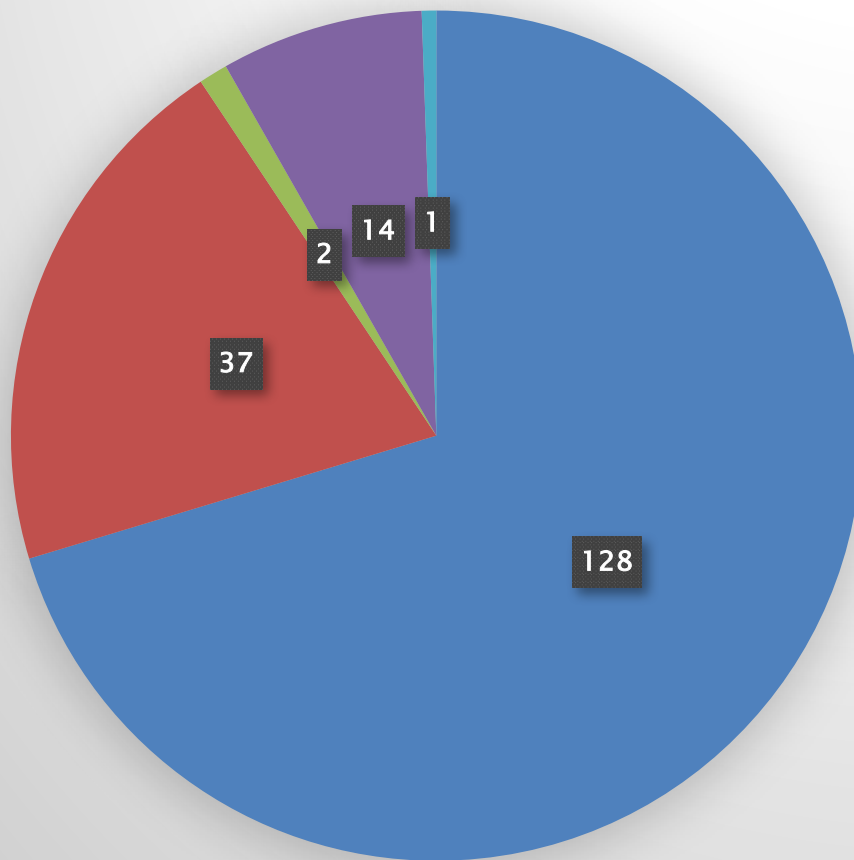
Q31:IdP運用に関するセキュリティポリシーが定められていますか？



- 1. 定められている。(以下に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

IDの運用状況

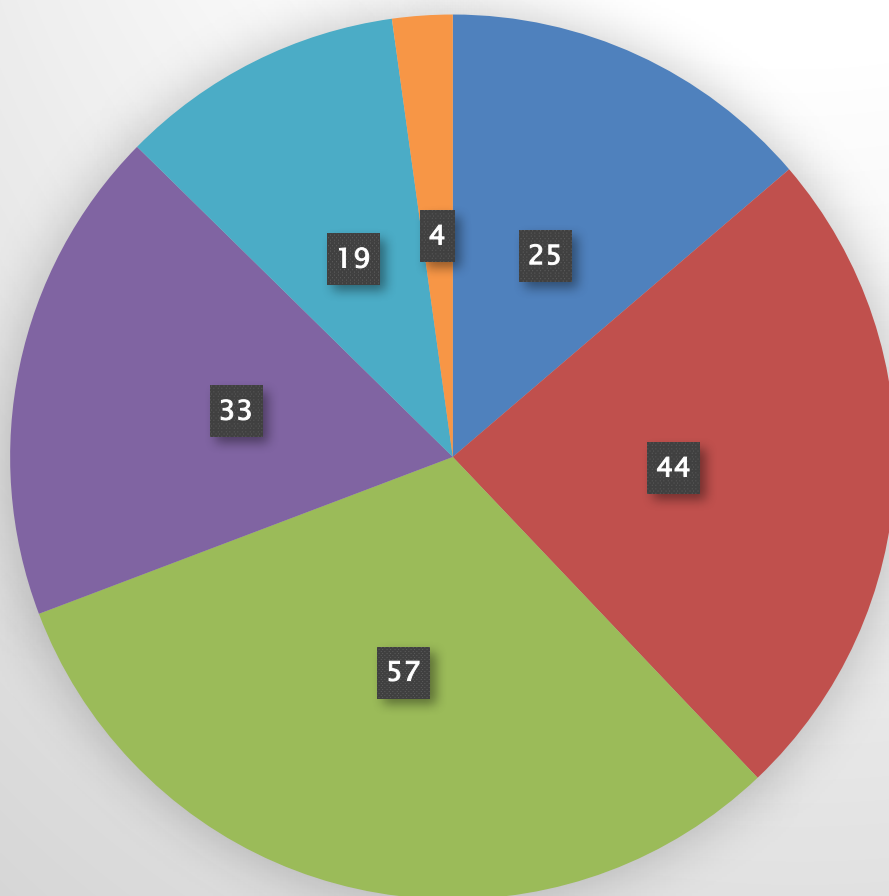
Q9:利用者IDは, 学務データや人事データ等, Trusted DB(組織にとって信頼できるデータベース)から作成されるように定めていますか? 選択肢からもっとも当てはまりのよいものを選んでください。



- 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。
- 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。
- 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やっている。
- 4. その他
- 記入なし

IDの運用状況

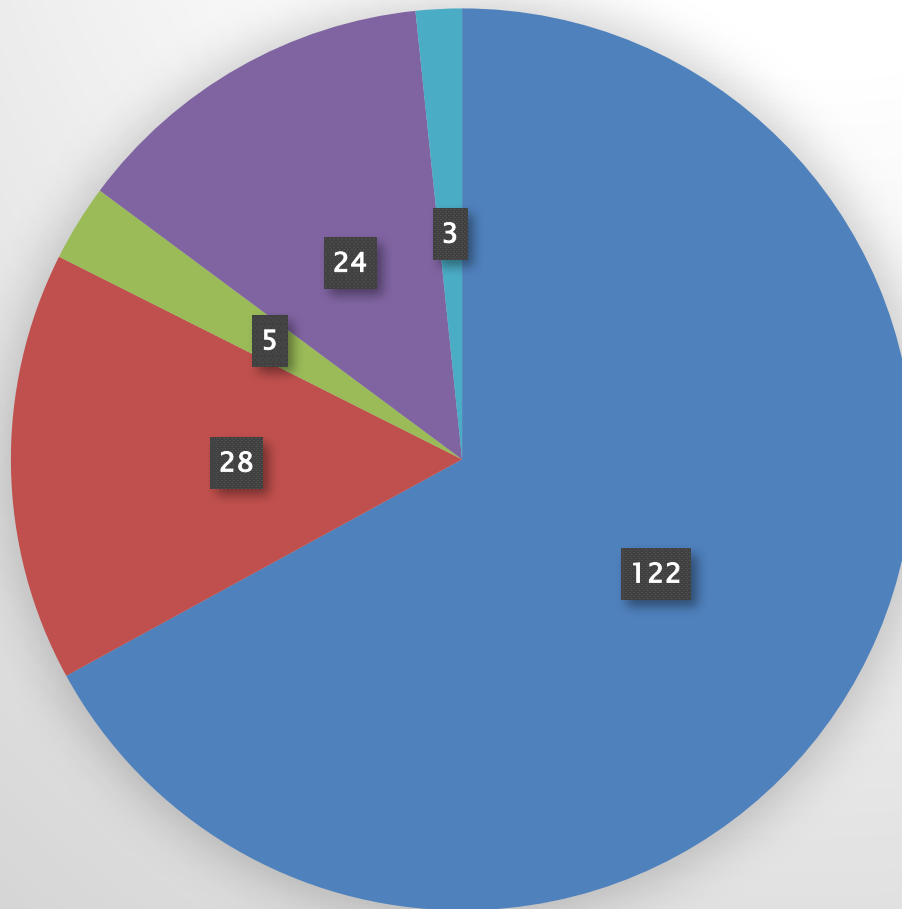
Q10:前項(Q9)を踏まえ, Trusted DBに含まれないものから利用者IDを作成する場合, どのようなルールで作成されていますか。



- 1. Trusted DBに登録した上でIDを発行する
- 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
- 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
- 4. 任意の手続きに沿って利用者IDを発行している
- 5. その他
- 記入なし

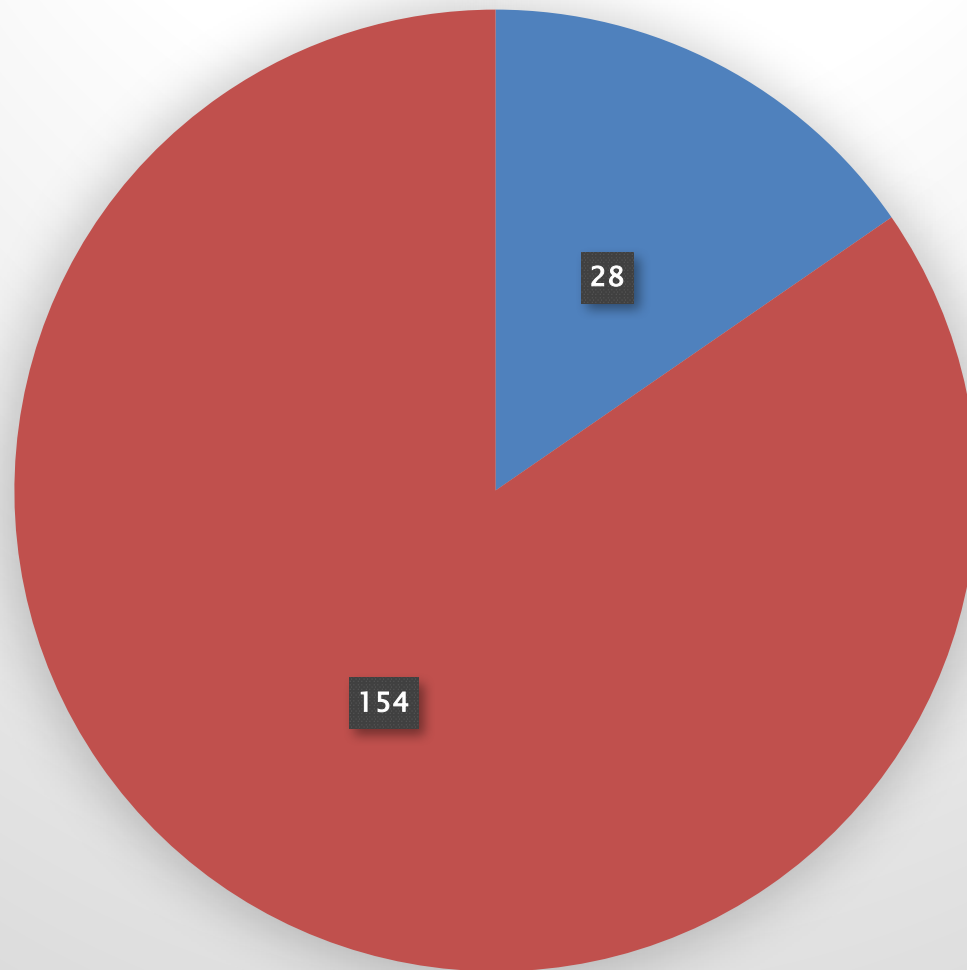
テクニカル —属性保証

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)

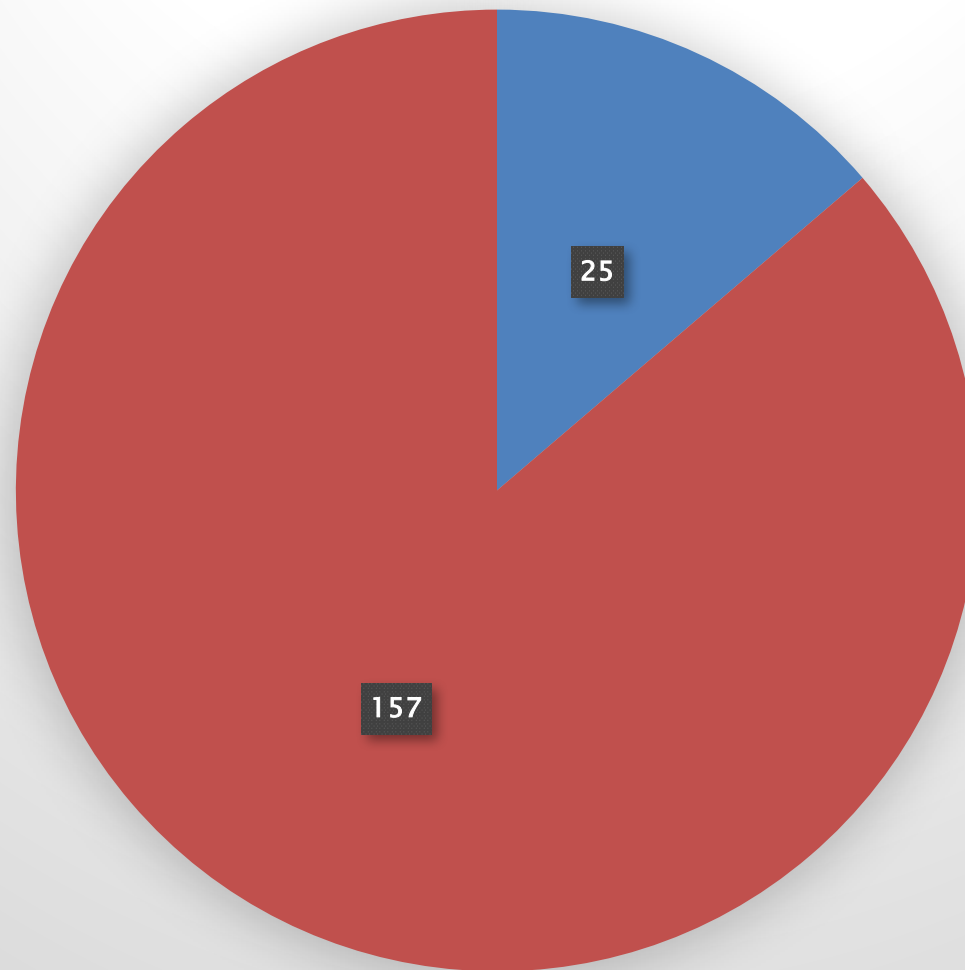


- 1. 利用者IDの属性は、Trusted DBの属性のみから計算されている。
- 2. 利用者IDの属性の一部には、Trusted DBの属性以外から生成されているものがある。
- 3. 利用者IDの属性は全て、Trusted DBの属性から生成されていない。
- 4. その他
- 記入なし

属性 O



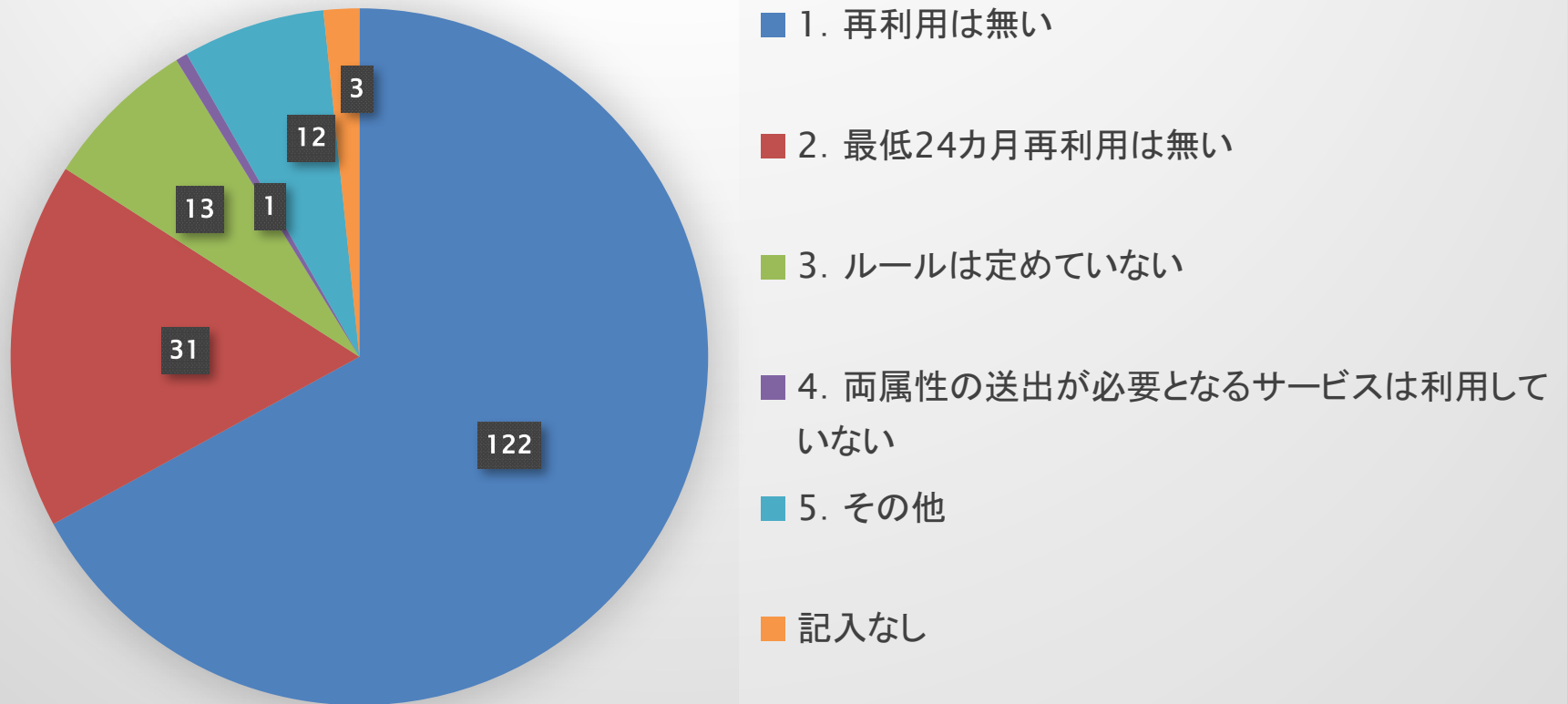
属性ePA



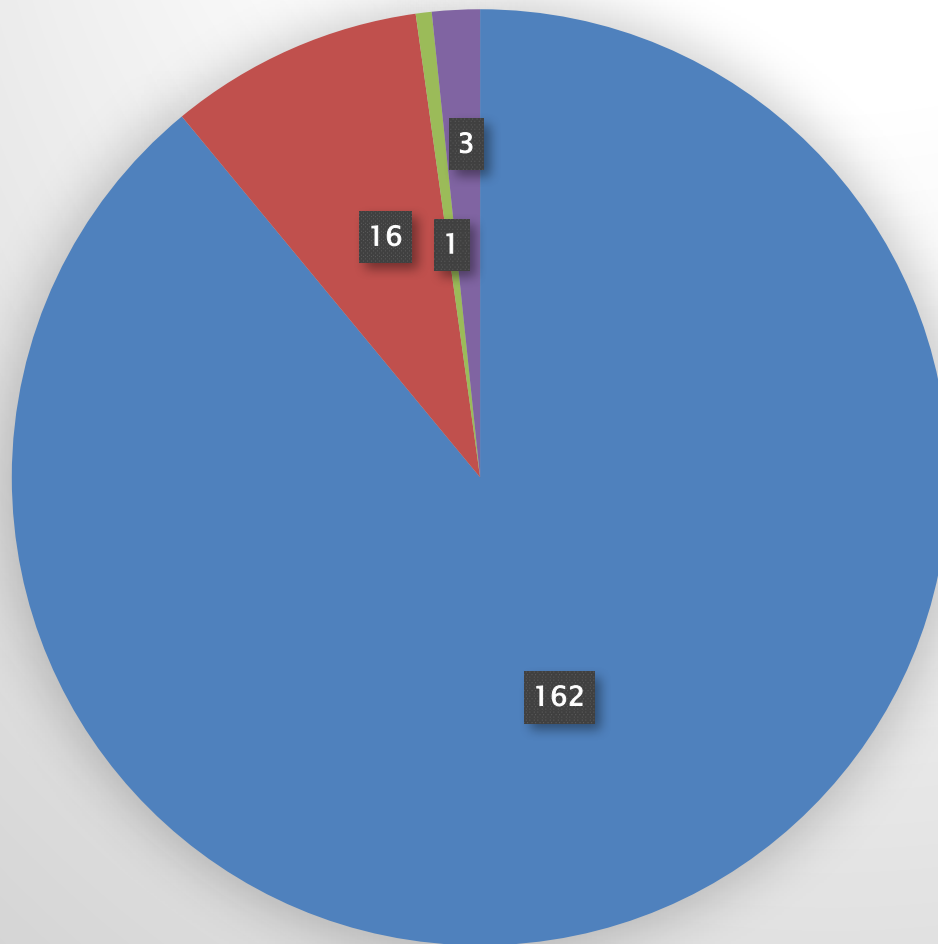
テクニカル IDの再利用

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）

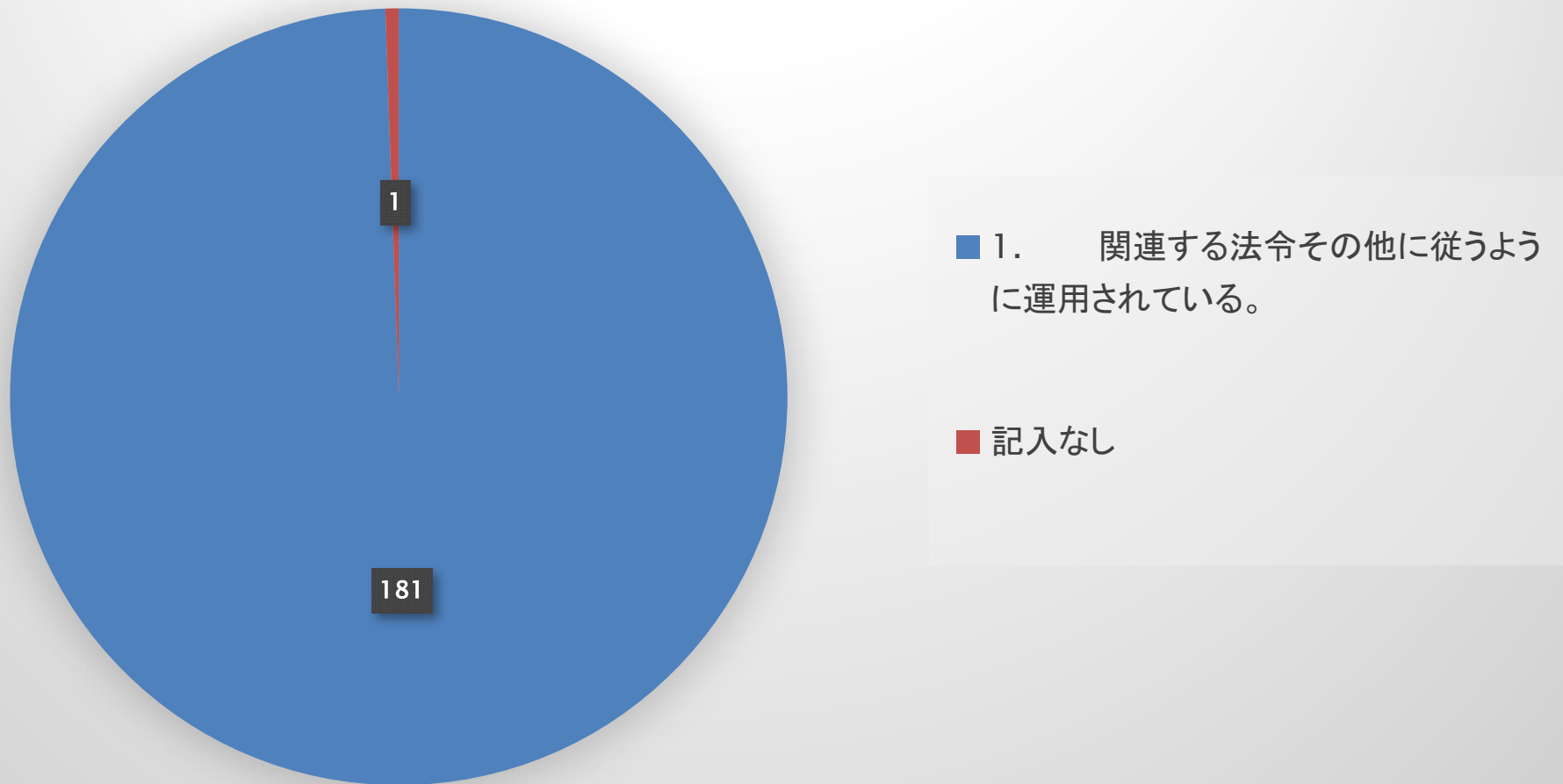


Q22:パスワードポリシーは定められていますか？



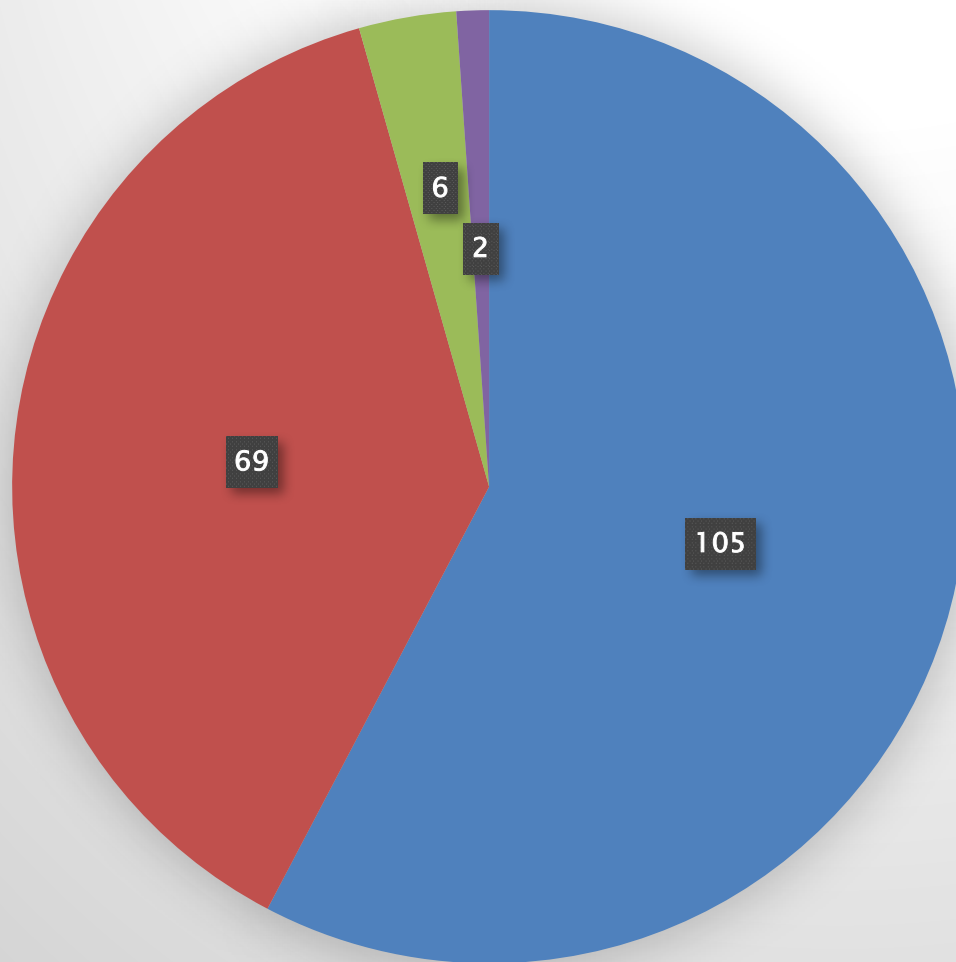
- 1. パスワードポリシーを定めている。
- 2. パスワードポリシーは定めていないが、啓蒙活動を積極的に行っている。
- 3. パスワードポリシーは定めておらず、特に啓蒙活動なども行っていない。
- 記入なし

Q25: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ますか？(実施要領10)



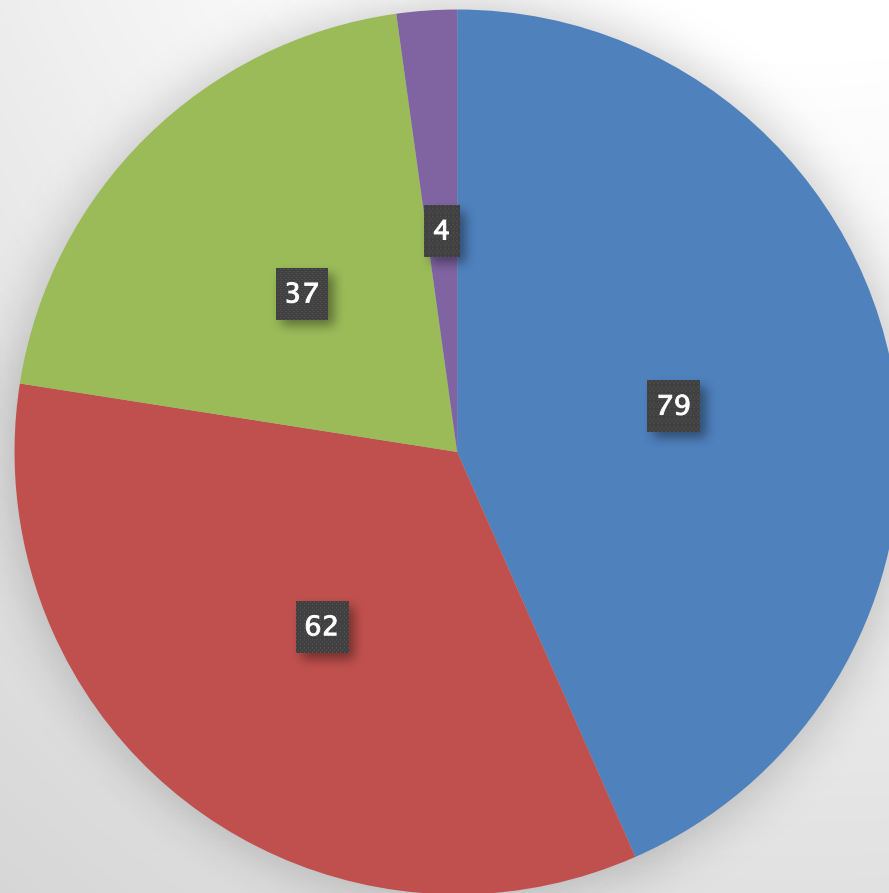
プライバシー — 規定の整備

Q26: プライバシーについて、具体的に規定はありますか？



- 1. プライバシーについての具体的な規定がある。
- 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。
- 3. プライバシーについての具体的な規定はない。
- 記入なし

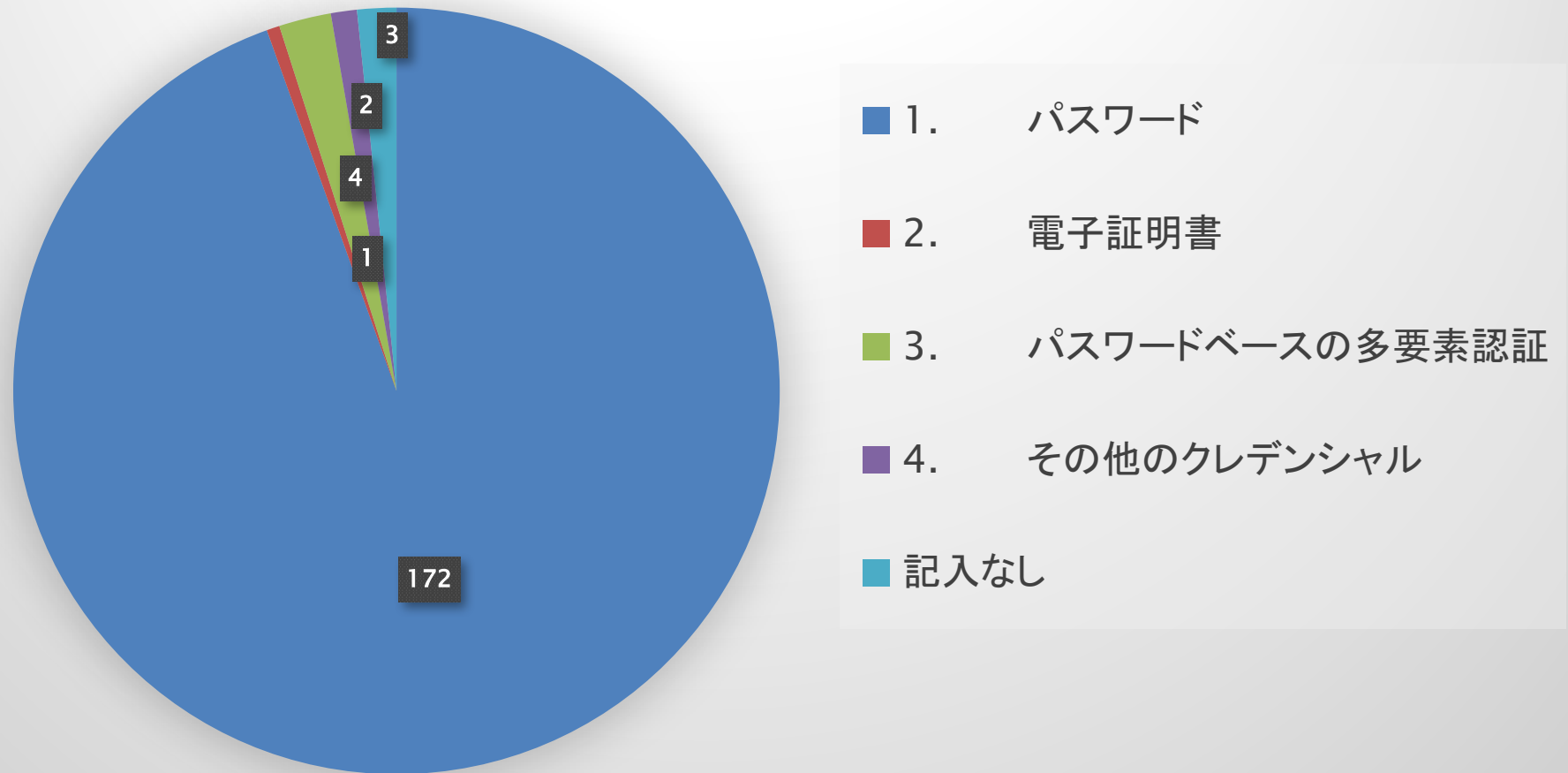
Q27:新たなSPのサービスを利用するとき、属性リリースの同意を得るためにuApproveもしくはその派生版を利用していますか？(技術運用基準8.6)



- 1. uApproveもしくはその派生版を利用している
- 2. uApproveおよびその派生版は利用していない
- 3. Shibboleth IdP Version3の属性リリース同意取得機能を使っている
- 記入なし

利用者IDのクレデンシャル

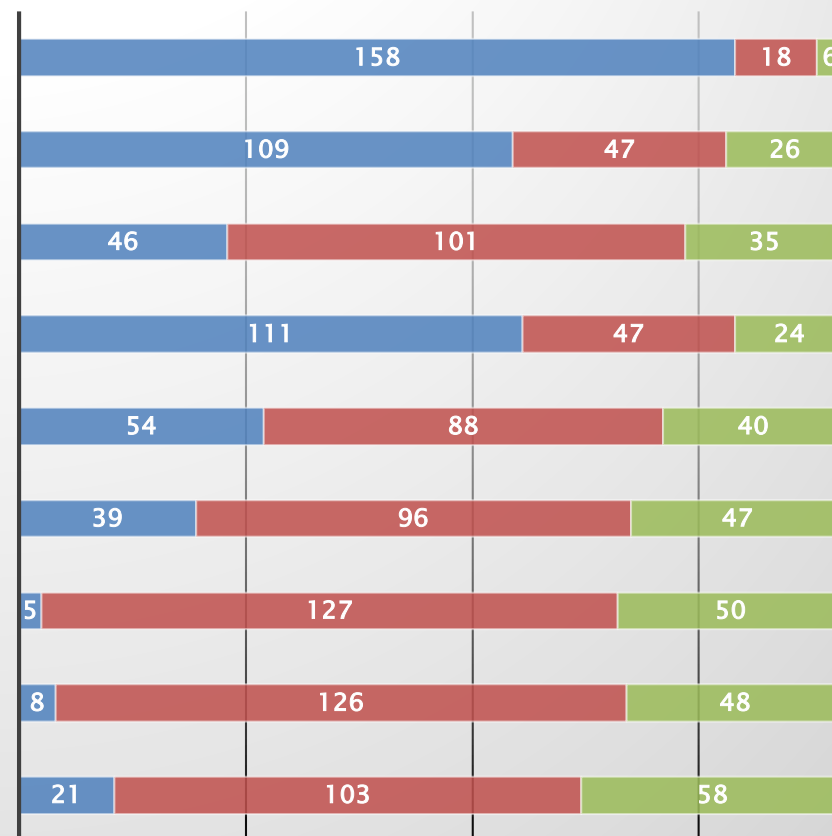
Q38:利用者IDとして利用している主なクレデンシャルの種類を教えてください。



クレデンシャルの安全性

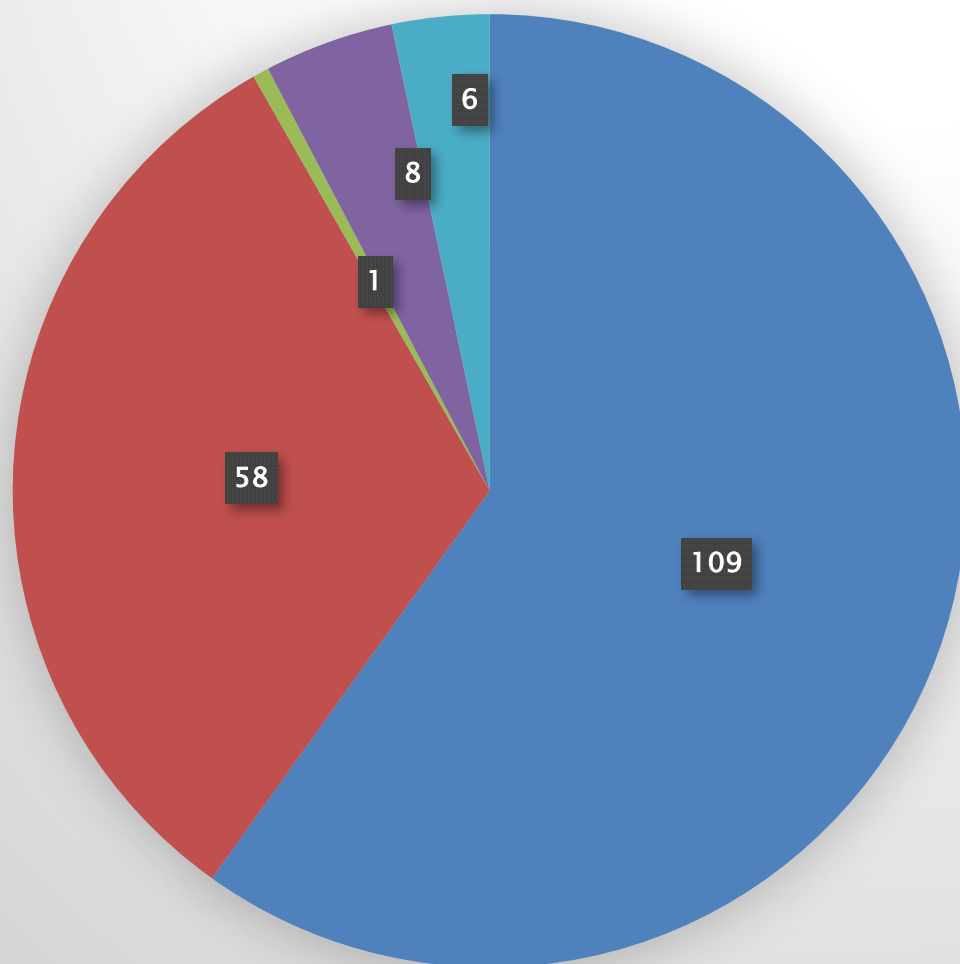
Q44:クレデンシャルの十分な安全性を実現する上で該当する取り組みがあれば教えてください。(複数回答可)

1. パスワードを8文字以上となるように推奨している。
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
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
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
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
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。
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。
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。
9. その他(具体的に記入)



■ ○ ■ × ■ 未選択

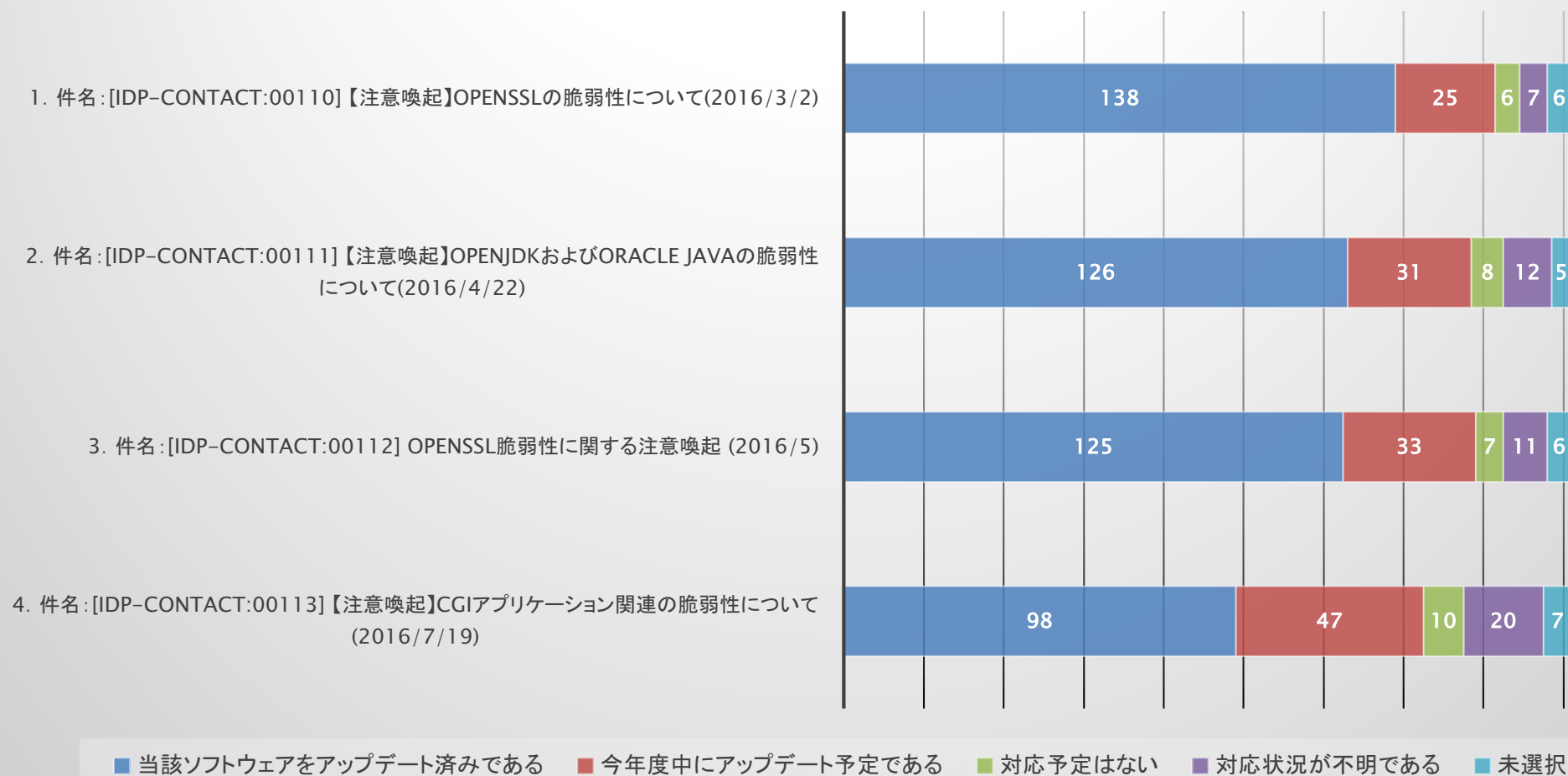
Q32:IdPの設定ファイルの管理はどのように行われていますか？



- 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
- 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
- 4. 設定ファイルの管理体制は不明である
- 5. その他
- 記入なし

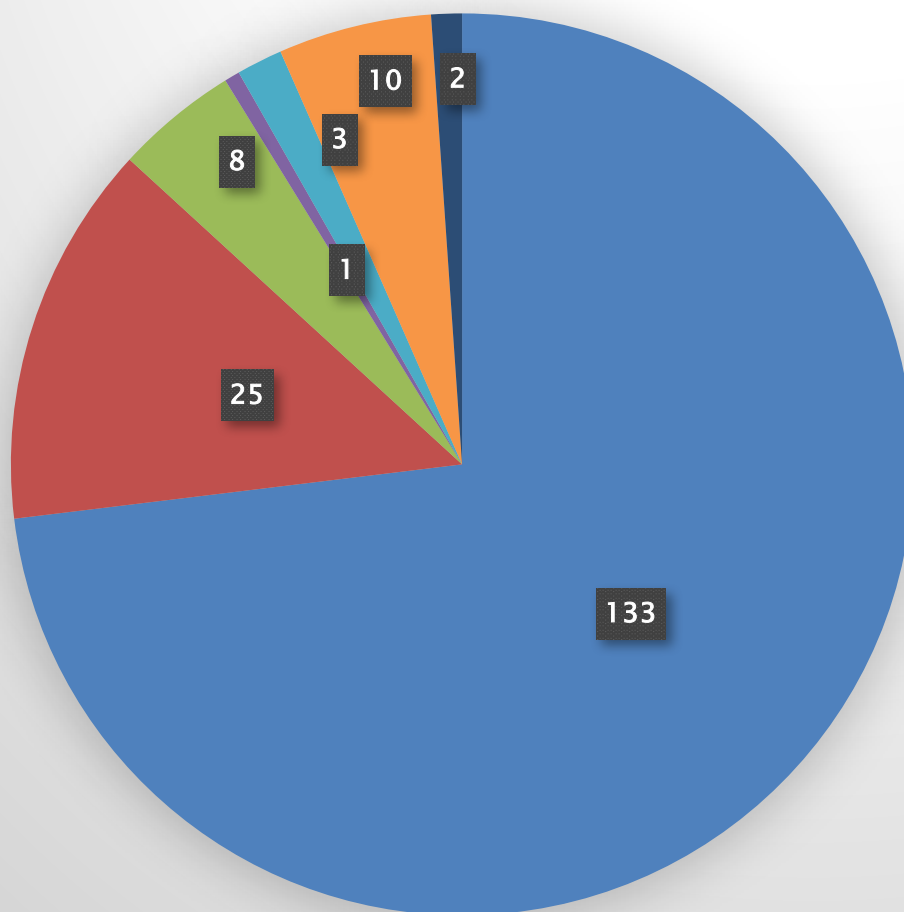
脆弱性への対応

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。



IdP v3へのアップデート状況

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
- 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



- ▶ 前年度に続き、高い水準でIdPが運用されていたことが読み取れます
- ▶ 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
- ▶ 引き続き、学認参加の各機関には、ご協力をお願い申し上げます

保証する属性について

