

# 2022年度学認参加 IdP 運用状況調査 総評

## 1 評価結果

---

調査への回答機関数は271件です。適切な運用を行っている機関が264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7件みられました。

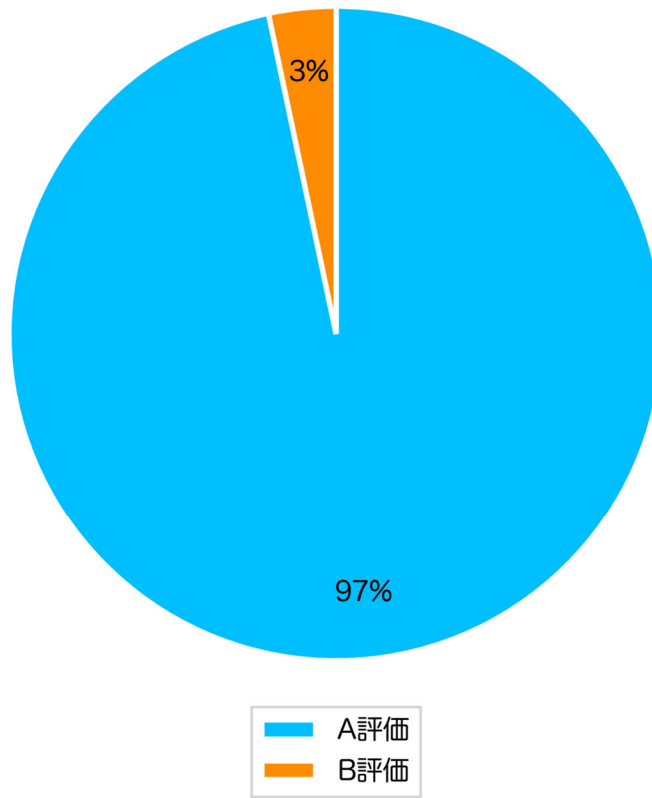
本調査の評価は、前年度同様、下記の基準で実施しました。

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 3系統がEOLを迎えたことによる、version 4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で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、3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。

A,B評価比率



	機関数
A 評価	264
B 評価	7

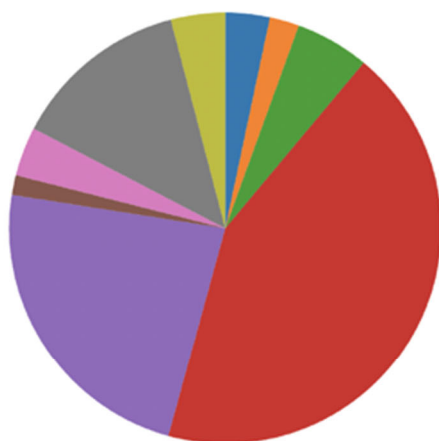
## 2 ガバナンス（規程の作成状況）

全学のセキュリティポリシーについては、247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24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については81件(30%)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、こちらから提示した規程が整備されているとの回答はあわせて183件ですが、その他と回答した11件についても、そのうちいくつかは他のなんらかの規程に準拠して運用されています。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

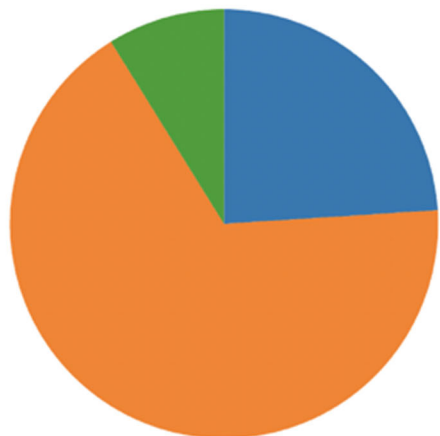
#### ■Q8■ IdP運用上での根拠規則や内規の制定状況について



- |   |     |       |
|---|-----|-------|
| 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】                 | 9   | (3%)  |
| 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】                 | 6   | (2%)  |
| 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。            | 15  | (6%)  |
| 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。           | 117 | (43%) |
| 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。                         | 63  | (23%) |
| 6. 規則などは特にないが、現在制定中である。                                 | 4   | (1%)  |
| 7. 全学的にはテスト利用の扱いになっている。                                 | 10  | (4%)  |
| 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。 | 36  | (13%) |
| 9. その他  | 11  | (4%)  |

### Q-30

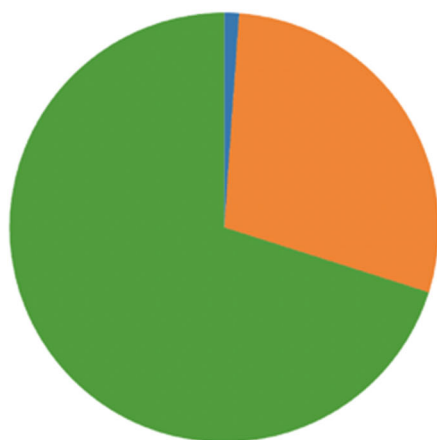
#### ■Q30■ 上位の全学または部局のセキュリティポリシーが定められ、それにしたがって運用されていますか？






- |                           |     |       |
|---------------------------|-----|-------|
| 1. 定められている。（下部にURLを記入）    | 65  | (24%) |
| 2. 定められているが、学内限定公開の扱いである。 | 182 | (67%) |
| 3. 特に定められていない。            | 24  | (9%)  |

## Q-31

■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)	3 ( 1%)	
2. 定められているが、学内限定公開の扱いである。	78 ( 29%)	
3. 特に定められていない。	190 ( 70%)	

### 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)

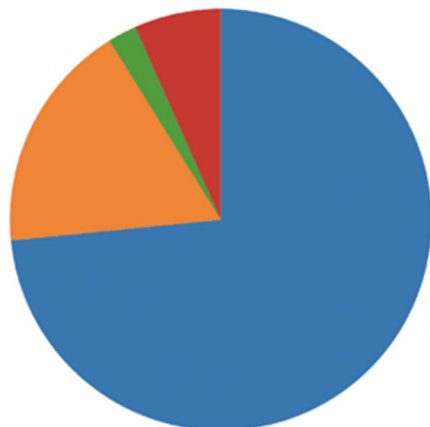
利用者 ID のソースとして、91%の機関で Trusted DB もしくは部局が責任をもって運用している DB をもとにしており、適切なユーザ管理がなされていることが読み取れます(Q9)。また、「その他」との回答においても、多くが書類による申請を実施していることが読み取れました。

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、情報系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

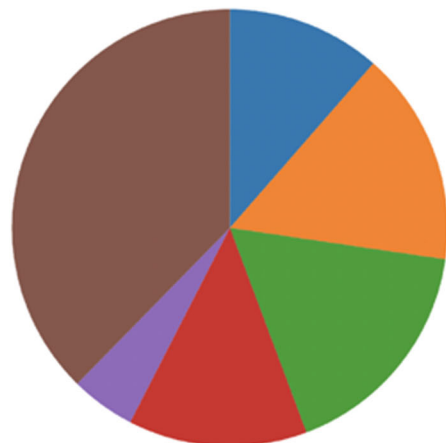
■Q9■ 利用者IDは、学務データや人事データ等、組織にとって信頼できるデータベースから作成されるように定めていますか？  
選択肢からもっとも当てはまりのよいものを選んでください。



1. 利用者IDのデータベースは、組織にとって信頼できるデータベースに基づいて作成されている。	199 (73%)	■
2. 利用者IDのデータベースは、組織にとって信頼できるデータベース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データベースから作られている。	48 (18%)	■
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。	6 (2%)	■
4. その他	18 (7%)	■

#### Q-10

■Q10■ 前項 (Q9) を踏まえ、組織にとって信頼できるデータベース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. 組織にとって信頼できるデータベースに登録した上でIDを発行する	31 (11%)	■
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	43 (16%)	■
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	46 (17%)	■
4. 任意の手続きに沿って利用者IDを発行している	36 (13%)	■
5. その他	13 (5%)	■
無回答	102 (38%)	■

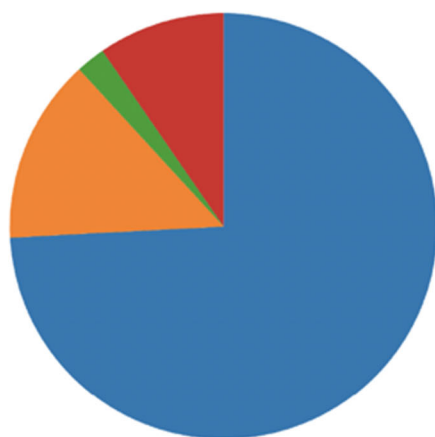
# 属性保証

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、技術運用基準 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、85%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。

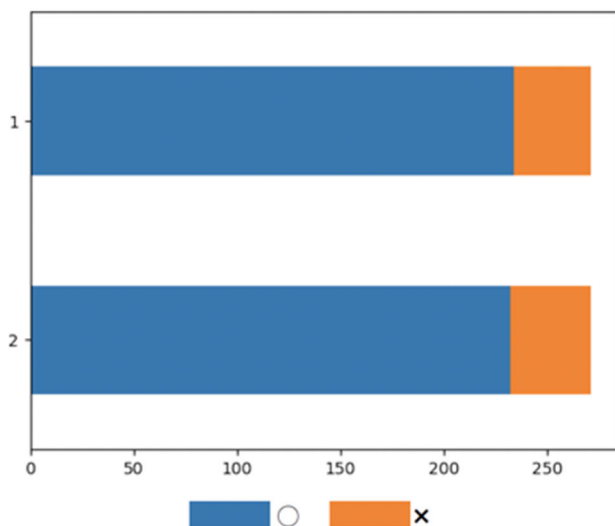
## Q-15

■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、組織にとって信頼できるデータベースの属性のみから計算されている。 201 (74%)
- 2. 利用者IDの属性の一部には、組織にとって信頼できるデータベースの属性以外から生成されているものがある。 38 (14%)
- 3. 利用者IDの属性は全て、組織にとって信頼できるデータベースの属性から生成されていない。 6 (2%)
- 4. その他 26 (10%)

### 保証する属性 (o,eduPersonAffiliation)



属性	○	×
1. eduPersonAffiliation	234	37
2. o	232	39

# パスワードポリシー

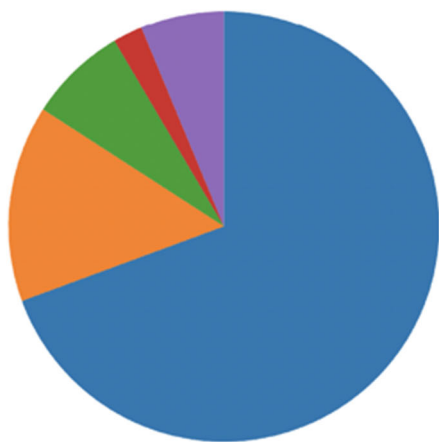
IDの再利用については、ごく少数のルールが定められていない機関を除き、再利用はないとの回答でした(Q19)。IDとクレデンシャルの配付については、本人確認を行うなど、各機関とも適切な運用が確立されています(Q20 自由記述より)。






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

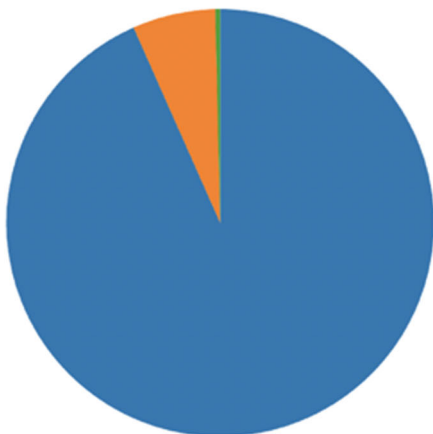
■Q19■ eduPersonPrincipalNameとeduPersonTargetedIDに関しては、かつて利用されていたものを再利用する場合は、最終の利用時から最低24ヶ月間隔をあけることを定めています。これを保証するために何が決められていますか？(技術運用基準8.2)






1. 再利用は無い	188 (69%)	
2. 最低24カ月再利用は無い	40 (15%)	
3. ルールは定めていない	20 (7%)	
4. 両属性の送が必要となるサービスは利用していない	6 (2%)	
5. その他	17 (6%)	

## Q-22

■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。	253 (93%)	
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。	17 (6%)	
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 (0%)	

## その他

ログの保存期間については、多くの大学が最低3ヶ月から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ヶ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）

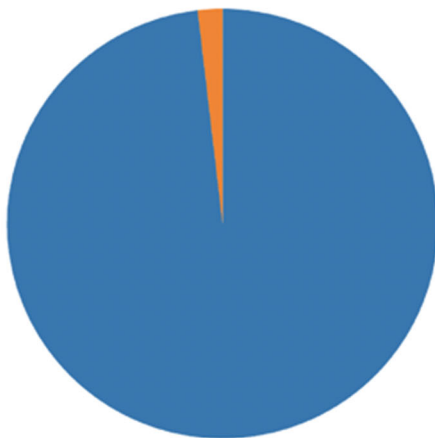
IdP から送信される個人情報については、5 件を除き、関係する法令に従うように運用されています (Q25)。「関連する法令その他に従うようには運用されていない」と回答した 5 機関については法令に従うよう働きかけていきます。



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 63% (Q26)、uApprove もしくは Shibboleth IdP に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 178 件（約 65%）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

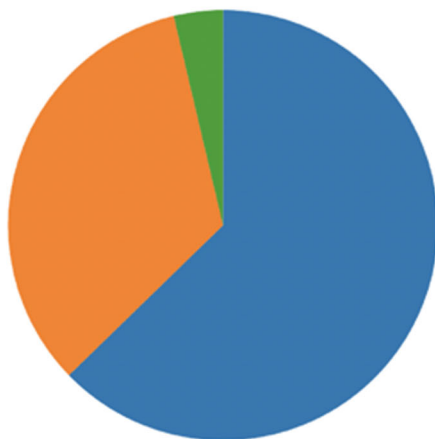
■Q25 ■ IdPから送信される個人情報について、関係する法令その他に 従うように運用されていますか？（実施要領10）






- |                              |            |   |
|------------------------------|------------|---|
| 1. 関連する法令その他に従うように運用されている。   | 266 ( 98%) |  |
| 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。 | 5 ( 2%)    |  |

### Q-26

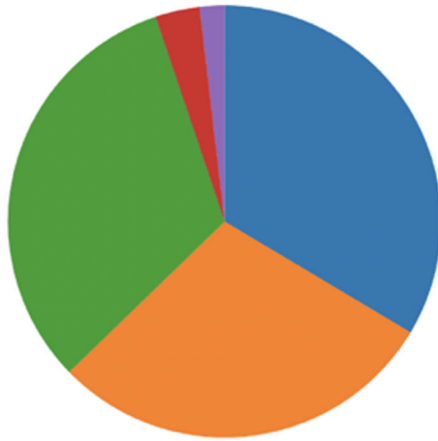
■Q26 ■ プライバシーについて、具体的に規定はありますか？








- |   |            |   |
|---|------------|---|
| 1. プライバシーについての具体的な規定がある。                        | 170 ( 63%) |  |
| 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。 | 91 ( 34%)  |  |
| 3. プライバシーについての具体的な規定はない。                        | 10 ( 4%)   |  |

# Q-27

■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	91 ( 34%)	
2.uApproveおよびその派生版は利用していない	79 ( 29%)	
3. Shibboleth IdP 組み込みの属性リリース同意取得機能を使っている	87 ( 32%)	
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	9 ( 3%)	
5. SimpleSAMLphp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	5 ( 2%)	

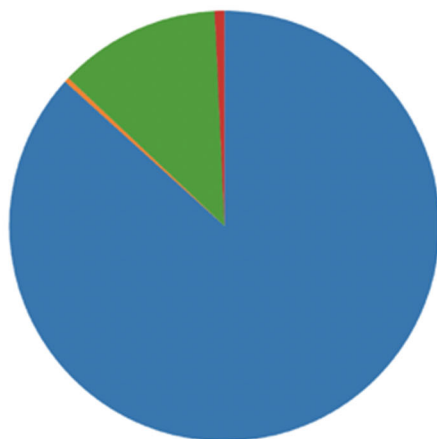
## 5 利用者 ID のクレデンシヤル

利用者 ID として利用している主なクレデンシヤルの種類 (Q38) としては、そのほとんど、87%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ヤル」との回答には学外からの認証についてパスワードベースの多要素認証を必須としている旨記述がありました。また1や3の回答の補足事項には、一部の成員やシステムに対して電子証明書・FIDO2・TOTPなどの多要素認証を行っているとの記述も見られました。段階的に多要素認証が展開されている様子が伺えます。

Q44は、クレデンシヤ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点を、ご認識いただきたいと思います。また、5のアカウントロックについては最近の Shibboleth IdP では設定により有効化できるようになっているなど、システムの機能についても固定的なものではないと捉え、定期的に見直していただくことを推奨します。

### Q-38

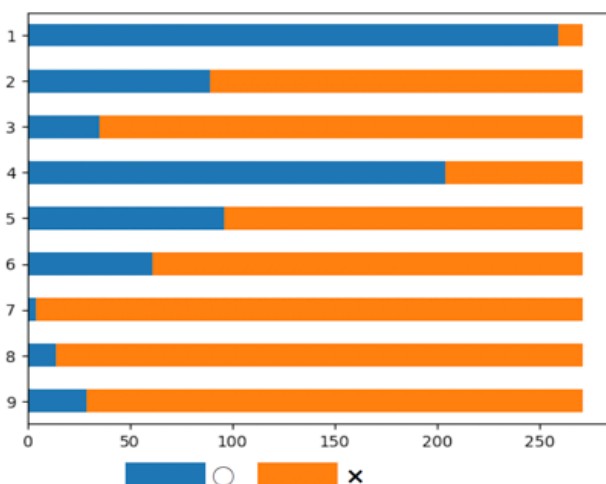
■Q38■ 利用者IDとして利用している主なクレデンシヤルの種類を教えてください。  
利用者IDの種類によって異なるクレデンシヤルを利用している場合、  
もしくは同一ID種で複数のクレデンシヤルを利用している場合は、  
主要な利用者ID種および主要なクレデンシヤルについて選んでいただいた上で、  
他のクレデンシヤルについては補足事項欄にて補足してください。



1. パスワード	235 ( 87%)	<span style="color: blue;">■</span>
2. 電子証明書	1 ( 0%)	<span style="color: orange;">■</span>
3. パスワードベースの多要素認証	33 ( 12%)	<span style="color: green;">■</span>
4. その他のクレデンシヤル	2 ( 1%)	<span style="color: red;">■</span>

### Q-44

■Q44■ クレデンシヤ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)



## 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 3 系統から 4 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 151 件 (56%)、設定変更を都度外部に依頼しているとしたものが 101 件 (37%) 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け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 3 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 の運用管理部門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。

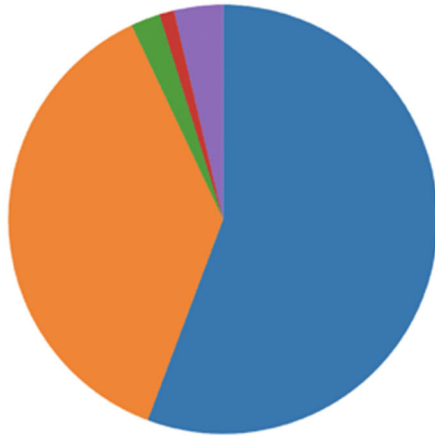
Q49 は、調査実施時点ですでにサポートが終了していた、Shibboleth IdP version 3 系統から、現行の Version 4 系統へのアップグレード状況についての質問です。調査実施時点でもまだ、46 の IdP で古いバージョンの Shibboleth IdP が稼働しているようです。






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 および 3 においては、今後アップデートおよび脆弱性情報は提供されないと明言されています。例外的に Version 2 は例外的に出された脆弱性情報<sup>1</sup>により脆弱性があることが確定しておりますが、これは Version 3 に脆弱性がないことを意味しておらず、EOL からの年月を考えれば別の脆弱性が存在することは十分考えられます。また、学認事務局からの技術情報は基本的に Version 4 に対して提供しており、古いバージョンは対象としません。

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。

<sup>1</sup> <https://www.gakunin.jp/ml-archives/upki-fed/msg01353.html> 参照

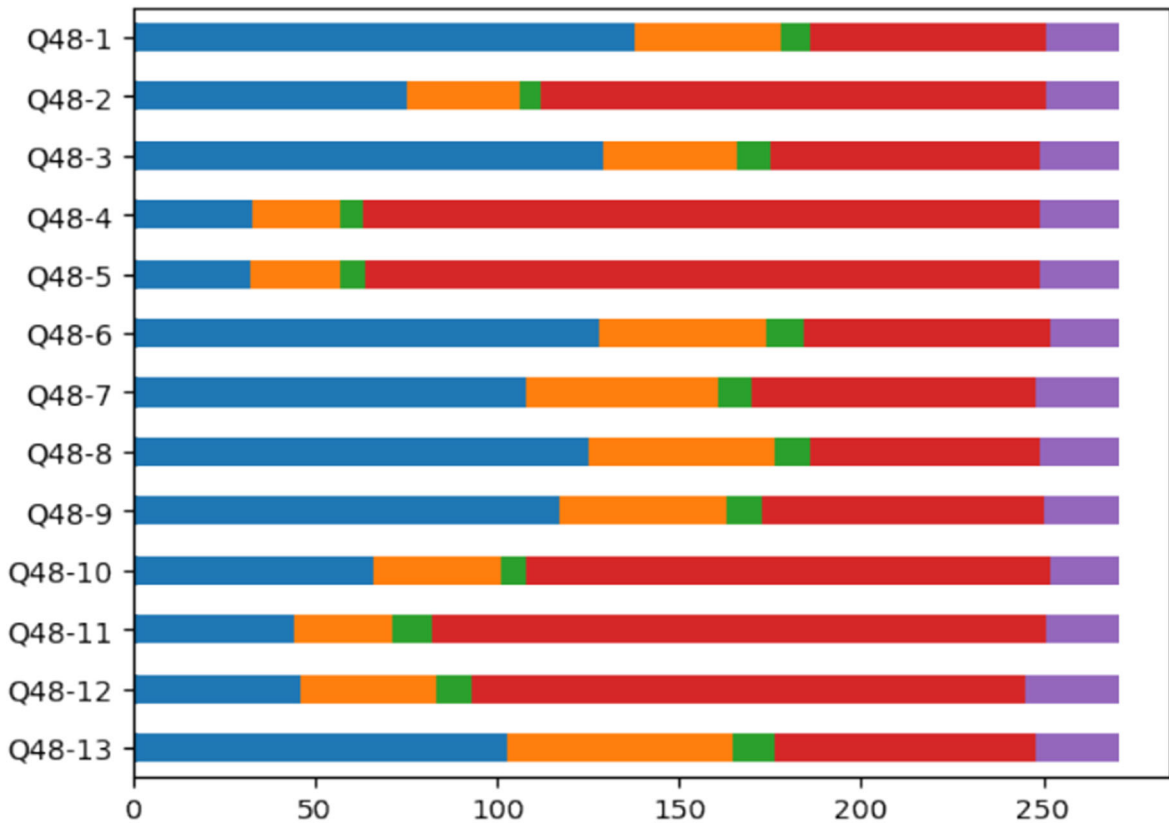
## ■Q32■ IdPの設定ファイルの管理はどのように行われていますか？



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	151（56%）	
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	101（37%）	
3. IDaaSに管理を全て委任している	6（2%）	
4. 設定ファイルの管理体制は不明である	3（1%）	
5. その他	10（4%）	

# Q-48

■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2021年10月以降に事務局からお知らせしたものです。

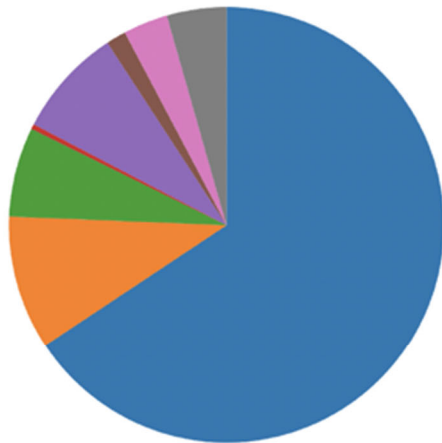


① 当該ソフトウェアをアップデート済である	② 今年度中にアップデート予定である	③ 対応予定はない	④ 対応不要だと判断した	⑤ 対応状況が不明である	
Q48-1	138	40	8	65	20
Q48-2	75	31	6	139	20
Q48-3	129	37	9	74	22
Q48-4	33	24	6	186	22
Q48-5	32	25	7	185	22
Q48-6	128	46	10	68	19
Q48-7	108	53	9	78	23
Q48-8	125	51	10	63	22
Q48-9	117	46	10	77	21
Q48-10	66	35	7	144	19
Q48-11	44	27	11	169	20
Q48-12	46	37	10	152	26
Q48-13	103	62	11	72	23

- Q48-1 [idp-contact:00232] [upki-fed:01445] 【注意喚起】 Apache HTTP Serverの脆弱性について (CVE-2021-40438) 2021/10/20 9:09:00
- Q48-2 [idp-contact:00233] [upki-fed:01446] 【注意喚起】 Apache Tomcatの脆弱性について(2021/10/14付アドバイザリ) 2021/10/20 9:09:55
- Q48-3 [idp-contact:00234] [upki-fed:01447] 【注意喚起】 Java SE JDK及びJREの脆弱性について(2021年10月) 2021/10/26 11:26:03
- Q48-4 [idp-contact:00247] [upki-fed:01470] 【注意喚起】 Shibboleth IdPのOIDC OPプラグインの脆弱性について(2022/1/3付アドバイザリ) 2022/1/14 14:12:27
- Q48-5 [idp-contact:00249] [upki-fed:01476] 【注意喚起】 Shibboleth IdPのOIDC OPプラグインの脆弱性について(2022/1/31付アドバイザリ) 2022/2/9 10:06:20
- Q48-6 [idp-contact:00249] [upki-fed:01476] 【注意喚起】 Shibboleth IdPのOIDC OPプラグインの脆弱性について(2022/1/31付アドバイザリ) 2022/2/9 10:06:20
- Q48-7 [idp-contact:00252] [upki-fed:01483] 【注意喚起】 OpenSSLの脆弱性について(2022/3/15付アドバイザリ) 2022/3/28 11:52:35
- Q48-8 [idp-contact:00253] [upki-fed:01484] 【注意喚起】 Apache HTTP Serverの脆弱性について (CVE-2022-22720) 2022/4/12 14:06:36
- Q48-9 [idp-contact:00258] [upki-fed:01492] 【注意喚起】 Java SE JDK及びJREの脆弱性について(2022年4月) 2022/4/27 9:21:53
- Q48-10 [idp-contact:00261] [upki-fed:01503] 【注意喚起】 Apache Tomcatの脆弱性について(2022/5/13付アドバイザリ) 2022/5/31 13:23:00
- Q48-11 [idp-contact:00264] [upki-fed:01509] 【続報】 【注意喚起】 字認Shibboleth IdP構築技術ガイドJetty版の設定例の問題につきまして 2022/7/1 11:47:09
- Q48-12 [idp-contact:00266] [upki-fed:01511] 【注意喚起】 Jettyの脆弱性について(2022/7/5付アドバイザリ) 2022/7/13 9:55:39
- Q48-13 [idp-contact:00267] [upki-fed:01513] 【注意喚起】 Java SE JDK及びJREの脆弱性について(2022年7月) 2022/8/2 10:14:55

## Q-49

■Q49■ すでにお知らせしている通り、Shibboleth IdP 3.x系は2020年12月でサポートが終了しました。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 4.x系統にアップグレード済みである	178 ( 66%)	
2. Shibboleth IdP 3.x系統が稼働しているが、 今年度内に4.x系統にアップグレード予定である	27 ( 10%)	
3. Shibboleth IdP 3.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	18 ( 7%)	
4. 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 ( 0%)	
5. Shibboleth IdP 以外のソフトウェアでIdPを運用している	22 ( 8%)	
6. 稼働しているソフトウェアは不明である	4 ( 1%)	
7. IDaaS( Identity as a Service )型のサービスを利用してIdPを運用している	9 ( 3%)	
8. その他 (具体的に記入)	12 ( 4%)	

本調査にご協力いただき、ありがとうございました。