令和 6 年 1 月 24 日
学術認証運営委員会
トラスト作業部会

2023 年度学認参加 IdP 運用状況調査 総評

内容

1 評価結果

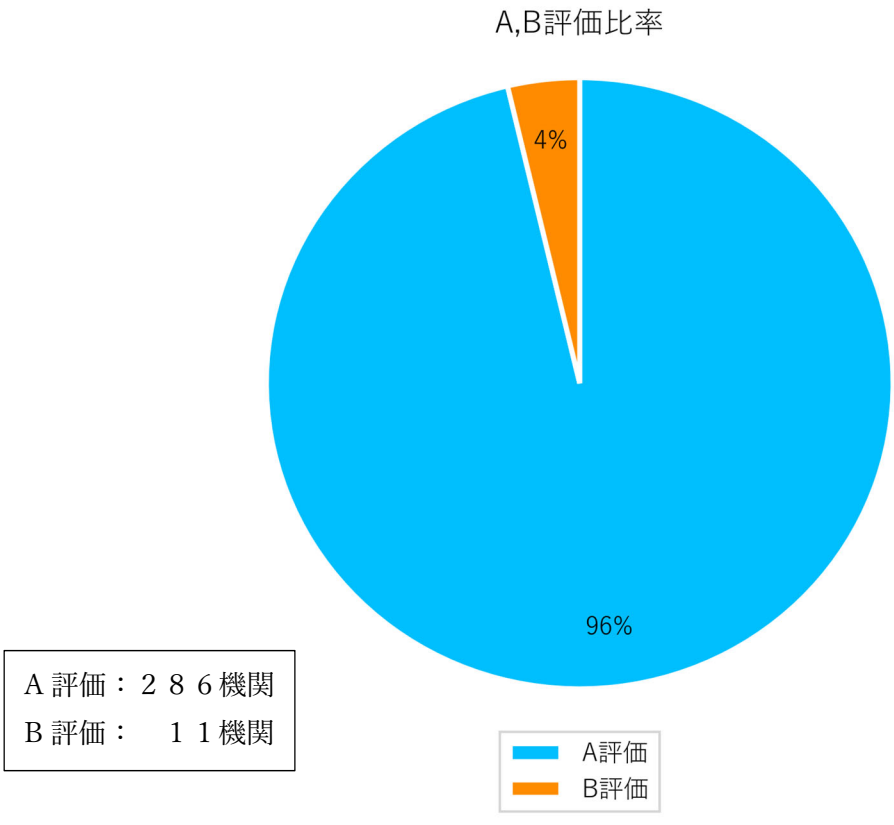
調査への回答機関数は 297 件です。適切な運用を行っている機関が 286 件となり、全体として良好な運用レベルです。一方、安定した運用のためには規程類の整備等が必要とみられる機関が 11 件（B 評価機関）みられました。

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 5 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、2 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。



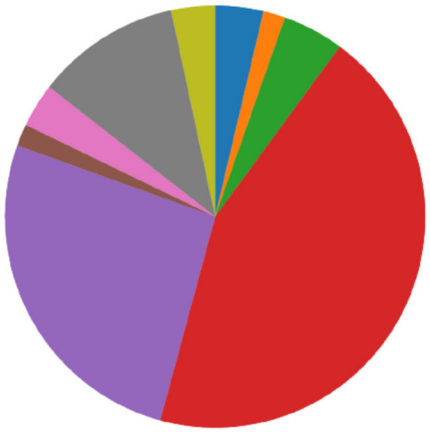
A 評価：	２８６機関
B 評価：	１１機関

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、272 件と 90%以上の機関で制定済みですが、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ついては 88 件（30%）が定められているとの回答でした(Q31)。

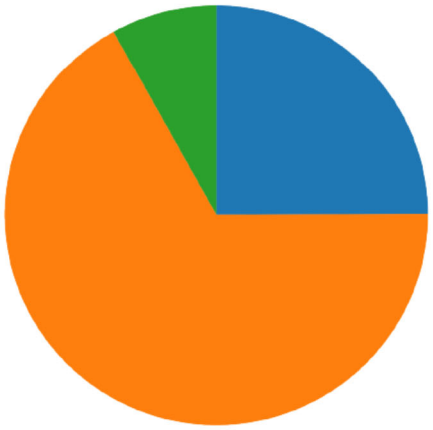
多くの機関において、利用者 ID の管理体制や全学的なセキュリティポリシーが整備されています。その基盤の上になりたって IdP が適切に運用されていることが読み取れます。Q8 において、こちらから提示した規程が整備されているとの回答はあわせて 194 件ですが、その他と回答した 10 件についても、そのうちいくつかは他のなんらかの規程に準拠して運用されています。前年度調査の結果に続き、半数以上の機関で整備されていると読み取ることができます。

■Q8■ IdP運用上での根拠規則や内規の制定状況について



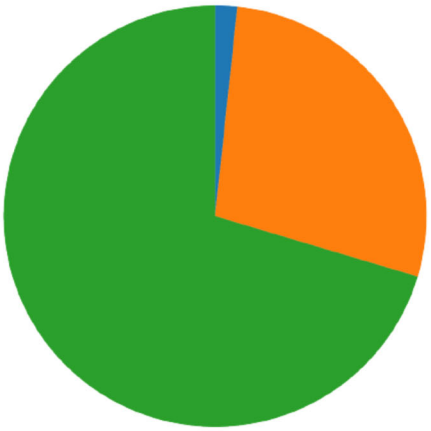
1. 全学情報サービスを担当する情報基盤センターの内規がある。【URLを記入】	11	(4%)
2. IdP運用規則，全学サービスセキュリティポリシーがある。【URLを記入】	5	(2%)
3. IdP運用規則，全学サービスセキュリティポリシーがあり，学内限定で公開されている。	14	(5%)
4. 全学サービスセキュリティポリシーが存在する。IdPはそのもとで適切に運用されている。	131	(44%)
5.特にないが，運用責任者の管理の下，適切に運用されている。	78	(26%)
6. 規則などは特にないが，現在制定中である。	5	(2%)
7. 全学的にはテスト利用の扱いになっている。	10	(3%)
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。	33	(11%)
9. その他	10	(3%)

■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。（以下にURLを記入）	74	(25%)
2.定められているが，学内限定公開の扱いである。	199	(67%)
3. 特に定められていない。	24	(8%)

■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？



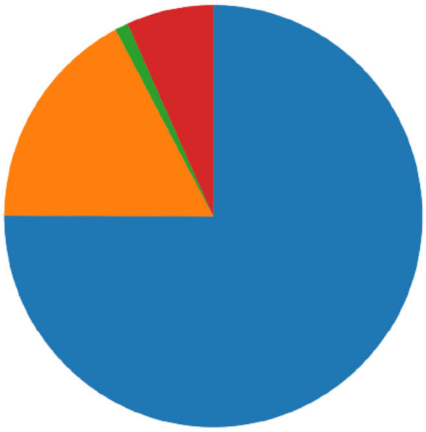
1. 定められている。（以下にURLを記入）	5 （ 2%）	
2.定められているが，学内限定公開の扱いである。	83 （28%）	
3. 特に定められていない。	209 （70%）	

3 テクニカルなこと

3.1 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、92%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の実施が読み取れました。
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。但し下記グラフは Q9 で 1 と回答した無回答数を集計していません)。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，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。	223	(75%)
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。	51	(17%)
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行っている。	3	(1%)
4. その他	20	(7%)

■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？

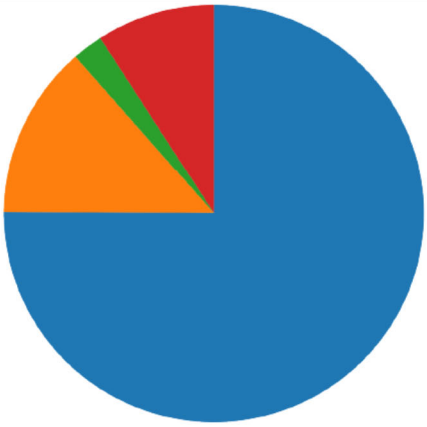
1. 組織にとって信頼できるデータベースに登録した上でIDを発行する	24	(16%)
2. 組織のアカウントを持たないユーザにはIDを発行しない	34	(23%)
3.情報セキュリティポリシーに基づき，利用者IDを作成している	38	(26%)
4. 任意の手続きに沿って利用者IDを発行している	38	(26%)
5. その他	13	(9%)

3.2 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。

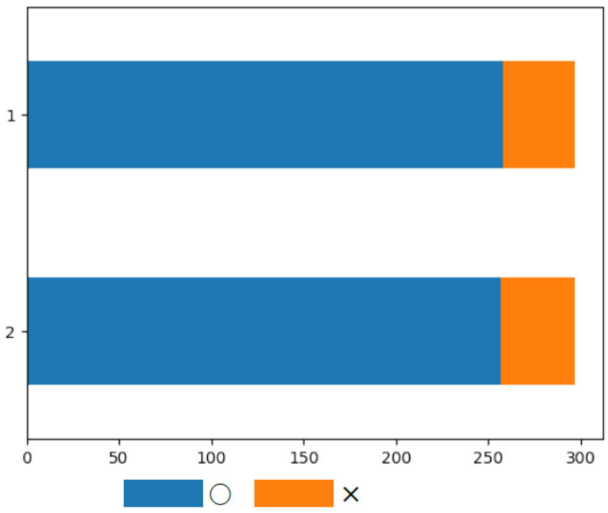
また今回も、前年度調査に引き続き、o と eduPersonAffiliation の状況に着目しました。両属性は、約87%の機関で組織として保証されていますが、「保証していない」としている機関がそれぞれ 13%程度残っています。学認の IdP は機関ごとに設置して参加申請されており、機関名は IdP として保証するべきです。送出できるよう設定してください。また実際に SP に送出し利用しているか否かにかかわらず、送出可能であれば「保証している」と回答してください。"faculty" ， "staff" ，"student"，"member"など、利用者の職位を表す eduPersonAffiliation についても同様です。

■Q15-1■ 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。	223	(75%)
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。	40	(13%)
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。	7	(2%)
4. その他	27	(9%)

■Q15-2■IdPにおいて組織が保証している属性について具体的にお答えください。
（IDの保証レベルに応じて将来のサービスの拡充に役立てることができます。）

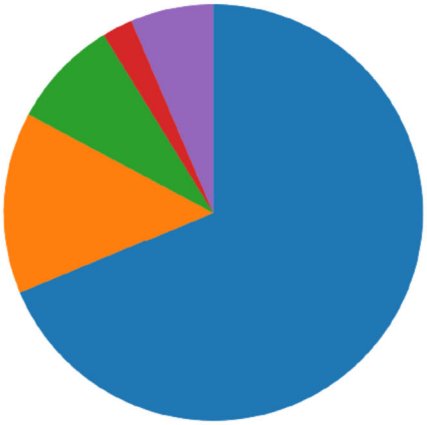


	○	×
1.eduPersonAffiliation	258	39
2.o	257	40

3.3 パスワードポリシー

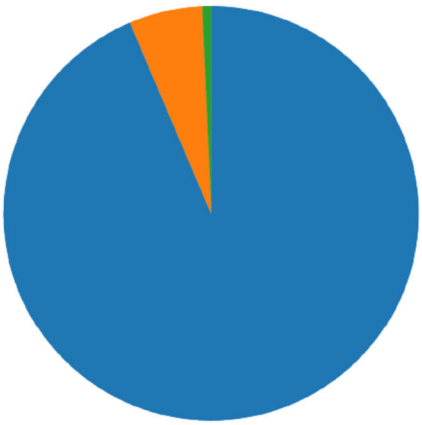
ID の再利用については、ごく少数のルールが定められていない機関を除き、再利用はないとの回答でした（Q19)。ID とクレデンシャルの配付については、本人確認を行うなど、各機関とも適切な運用が確立されています(Q20 自由記述より)。
共有 ID の禁止に関しても、各機関にて、規定での禁止、セキュリティ面からの啓蒙活動や、共有しなくても業務を行えるような運用が行われていることが読み取れました(Q21 自由記述より)。パスワードポリシーについては、94%の機関でパスワードポリシーがある、6%の機関でポリシーはないが啓蒙活動はしている、との回答でした(Q22)。

■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	204 (69%)	
2. 最低24カ月再利用は無い	42 (14%)	
3. ルールは定めていない	25 (8%)	
4. 両属性の送出が必要となるサービスは利用していない	7 (2%)	
5. その他	19 (6%)	

■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。	278 (94%)	
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。	2 (1%)	

3.4 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)。

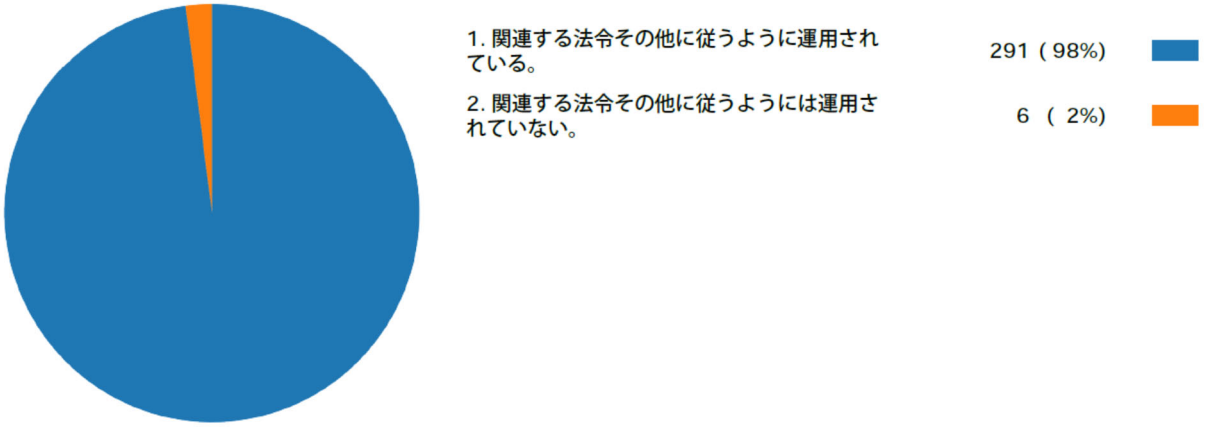
4 プライバシー（プライバシーに関係すること）

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 6 機関については法令に従うよう働きかけていきます。

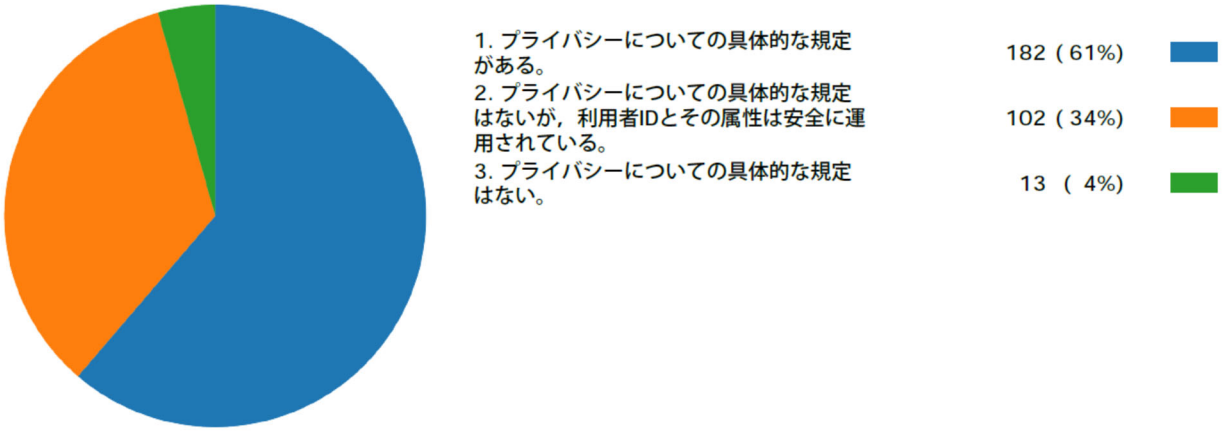
また、プライバシーについて具体的な規則を制定している機関は前年から微減の 61%(Q26)、uApprove、Shibboleth IdP 及び同等機能に搭載された属性リリース同意取得機能を利用していると回答した機関は 213 件（約 72%）でした(Q27)。

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。

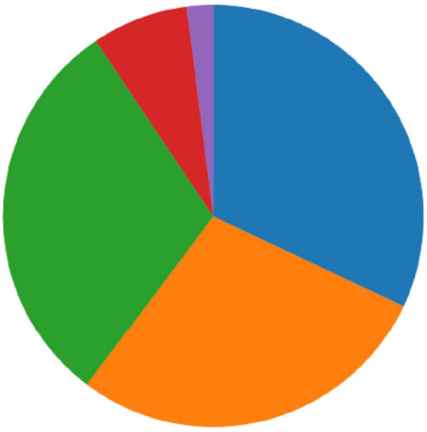
■Q25■ IdPから送信される個人情報について，関係する法令その他に従うように運用されていますか？（実施要領12）



■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）



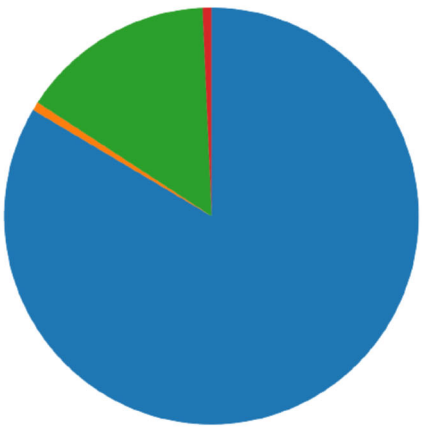
1.uApproveもしくはその派生版を利用している	95（32%）	
2.uApproveおよびその派生版は利用していない	84（28%）	
3. Shibboleth IdP 組み込みの属性リリース同意取得機能を使っている	90（30%）	
4. IDaaSに組み込まれている属性リリース同 意取得機能を使っている	22（ 7%）	
5. SimpleSAMLphpに組み込まれてい る属性リリース同意取得機能を使っている	6（ 2%）	

5 利用者 ID のクレデンシャル

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、84%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ャル」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。

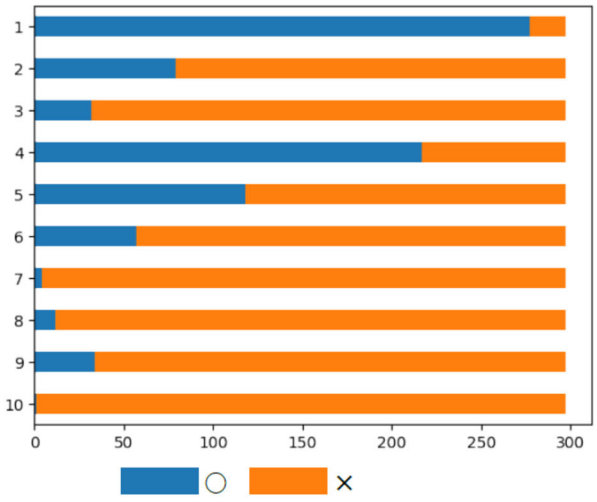
Q44 は、クレデンシャルの安全性を実現するために実施している取り組みについて質問したものです。現状の把握を目的としたものですが、設問中のいくつかは、NIST SP800-63-3 において、非推奨とされているものがあります。無論、ここで○と回答したものが誤りであるということではなく、現在、機関で定められている規程類に該当する記述がある場合、それは守られるべきものです。注視すべきは、策定時には正しいとされていたものが、取り巻く制度的、あるいは技術的状況によって変化していく可能性があるという点です。規程類は一度定めたらそれでよいものではなく、継続的なメンテナンスを行っていく必要があるものだということを、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。

■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。
（ここでいうパスワードには,デバイス側で保持し認証が完結するPINを含めないものとします。） 利用者IDの種類によって異なるクレデンシャ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ャ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ャルについて選んでいただいた上で，他のクレデンシャ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	248	(84%)
2. 電子証明書	2	(1%)
3. パスワードベースの多要素認証	45	(15%)
4. その他のクレデンシャル	2	(1%)

■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）



	○	×
1. パスワードを8文字以上となるように推奨している。	277	20
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。	79	218
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。	32	265
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。	217	80
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。	118	179
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。	57	240
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。	4	293
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。	12	285
9. その他（具体的に記入）	34	263
該当するものはない	1	296

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 5 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 161 件（54%）、設定変更を都度外部に依頼しているとしたものが 111 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れば問題はありません。IDaaS での管理も同様です。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（「不要だと判断」を含む）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 系統やサポート終了予定の Version 4 系統から、現行の Version 5 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、24 機関での Version 3 系統が、163 機関で Version 4 系統の 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。

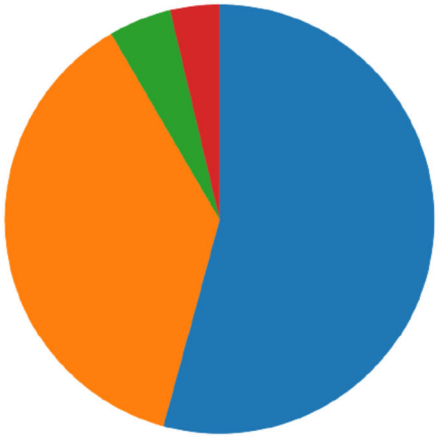
Shibboleth IdP version 2 および 3 においては、今後アップデートおよび脆弱性情報は提供されないと明言されています。例外的に Version 2 は例外的に出された脆弱性情報[1]により脆弱性があることが確定しておりますが、これは Version 3 に脆弱性がないことを意味しておらず、EOL からの年月を考えれば別の脆弱性が存在することは十分考えられます。また、学認事務局からの技術情報は基本的に Version 4 及び Version 5 に対して提供しており、古いバージョンは対象としません。

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。

---

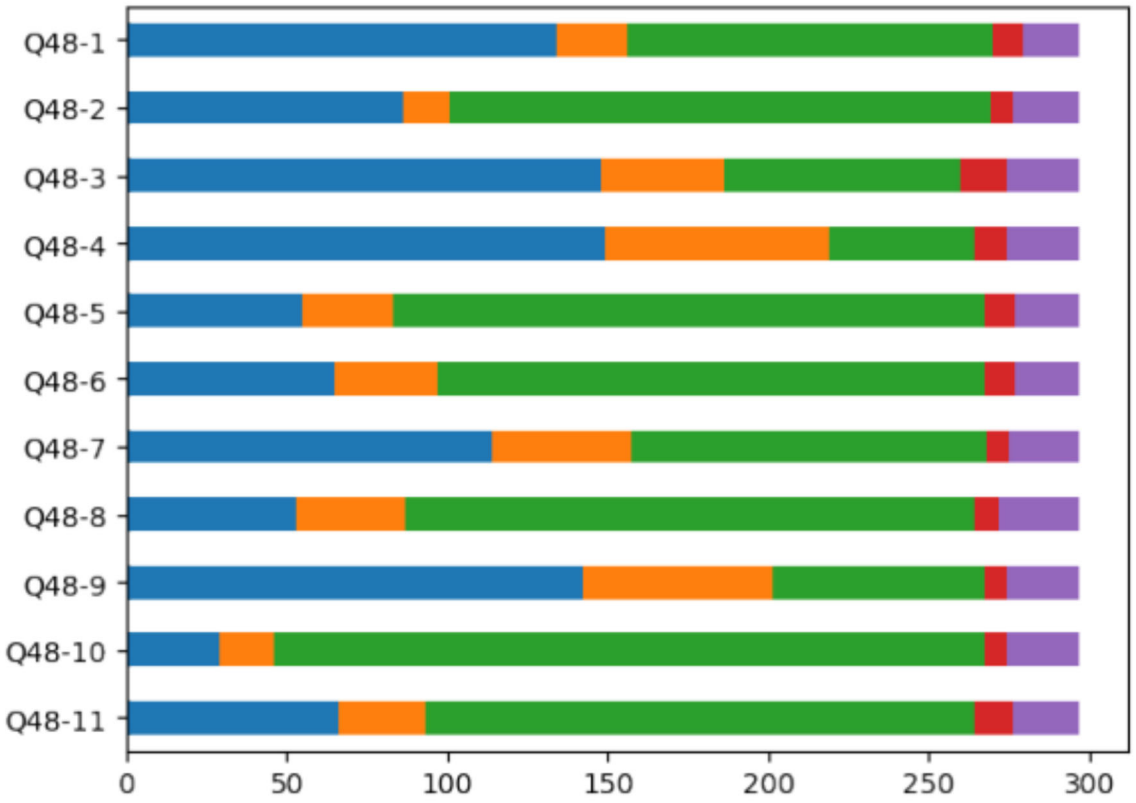
[1] https://www.gakunin.jp/ml-archives/upki-fed/msg01353.html 参照

■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	161（54%）	
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	111（37%）	
3. IDaaSに管理を全て委任している	14（5%）	
5. その他	11（4%）	

■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2022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 対応不要だと判断した
④ 対応予定はない
⑤ 対応状況が不明である

	①	②	③	④	⑤
Q48-1	134	22	114	9	18
Q48-2	86	15	168	7	21
Q48-3	148	38	74	14	23
Q48-4	149	70	45	10	23
Q48-5	55	28	184	10	20
Q48-6	65	32	170	10	20
Q48-7	114	43	111	7	22
Q48-8	53	34	177	8	25
Q48-9	142	59	66	7	23
Q48-10	29	17	221	7	23
Q48-11	66	27	171	12	21

Q48-1 [upki-fed:01520]【注意喚起】Apache Tomcatの脆弱性について(2022/9/28付アドバイザリ) 2022/10/07 09:21:41

Q48-2 [upki-fed:01527]【注意喚起】OpenSSLの脆弱性について(2022/11/1付アドバイザリ) 2022/11/21 16:54:00

Q48-3 [upki-fed:01534]【注意喚起】Shibboleth IdPの脆弱性について(2022/12/16付アドバイザリ)2022/12/21 13:34:20

Q48-4 [upki-fed:01549]【注意喚起】OpenSSLの脆弱性について(2023/2/7付アドバイザリ)2023/2/21 11:54:20

Q48-5 [upki-fed:01556]【注意喚起】Shibboleth IdPの脆弱性について(2023/3/30付アドバイザリ) 2023/4/10 13:11:21

Q48-6 [upki-fed:0]【注意喚起】Apache Tomcatの脆弱性について(2023/3/22付アドバイザリ)2023/4/19 11:28:24

Q48-7 [upki-fed:1]【注意喚起】Apache HTTP Serverの脆弱性について (CVE-2023-25690)2023/4/25 14:41:29

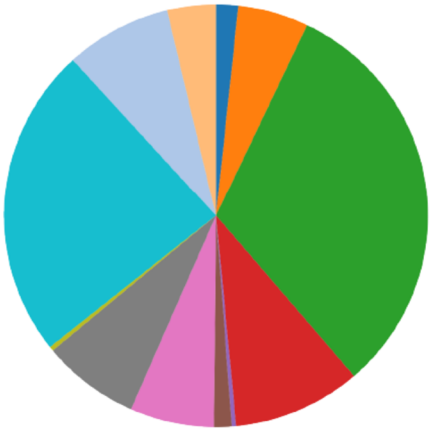
Q48-8 [upki-fed:2]【注意喚起】Jettyの脆弱性について(2023/4/18付アドバイザリ) 2023/5/8 14:19:08

Q48-9 [upki-fed:3]【注意喚起】Java SE JDK及びJREの脆弱性について(2023年4月)2023/5/9 16:46:43

Q48-10 [upki-fed:5]【注意喚起】Shibboleth IdPのOIDC OPプラグインの脆弱性について(2023/5/12付アドバイザリ)2023/5/19 10:06:46

Q48-11 [upki-fed:16]【注意喚起】Apache Tomcatの脆弱性について(2023/6/21付アドバイザリ)2023/6/28 14:43:52

■Q49■ 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。 ただし,アプライアンス製品ないしIDaaS (IDentity as a Service) 型のクラウドサービスを利用している場合はその旨回答し,Q49-bに詳細を記入してください。 (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。Shibboleth IdP 4.x 系は2024年9月1日にサポート終了予定です。) 技術運用基準では推奨項目になっています。（技術運用基準2.3）



1. Shibboleth IdP 5.x系統にアップグレード済みである	5	(2%)
2. Shibboleth IdP 4.x系統が稼働しているが，今年度内に5.x系統にアップグレード予定である	16	(5%)
3. Shibboleth IdP 4.x系統が稼働しているが，来年度かつサポート終了までに5.x系統にアップグレード予定である	94	(32%)
4. Shibboleth IdP 4.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（サポート終了後のアップグレード予定を含む）	29	(10%)
5. Shibboleth IdP 3.x系統が稼働しているが，今年度内に5.x系統にアップグレード予定である	1	(0%)
6. 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	4	(1%)
7. 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（来年度以降のアップグレード予定を含む）	19	(6%)
8. Shibboleth IdP以外のソフトウェアでIdPを運用している	22	(7%)
9. 稼働しているソフトウェアは不明である	1	(0%)
10.アプライアンス製品を利用してIdPを運用している	71	(24%)
11.IDaaS(IDentity as a Service)型のクラウドサービスを利用してIdPを運用している	24	(8%)
12. その他（具体的に記入）	11	(4%)

本調査にご協力いただき、ありがとうございました。