【2026年度】学認参加IdP運用状況調査にご協力いただきましてありがとうございます

本調査は必須マークがついている設問は回答必須です。 また，必須マークのない設問についても，対象となる場合は，必ずご回答ください。 本調査にご回答いただく際，担当がわかれている場合は，適宜当該部門に確認の上ご回答ください。

IdPの運用には下記の各部門が関係する可能性があります（機関によって異なります）。 またIdPの運用を外部委託している場合，当該委託事業者やIDaaS事業者が下記いずれか，または複数を担当している場合があります。

設問のまとまりごとに，関係すると思われる部門（IdP運用担当部門以外）を記入しておりますが，照会先をこれに限定するものではありません。

なお今年度の調査は，設問1～47まで，2025年度と同様の設問を設定しております。前年度調査票をご参照の上ご回答ください。 前年度調査票は こちら からご参照いただけます（ただし今年度から新たに調査に参加いただいた機関については参照いただけません）。

● IdP運用担当部門・・・多くの場合，IdP運用担当者の所属部門が該当します。

▲ ID基盤管理部門・・・LDAP やActive DirectoryなどのID基盤を管理する部門が該当します。 情報基盤センター等以外にも，人事や総務が担当している場合があります。

▼ システム管理部門・・・IdPの設定とインフラを管理する部門が該当します。 情報基盤センター等以外に，図書館などが担当している場合があります。

＊ポリシー管理部門・・・機関の規程やセキュリティポリシーなどを管理する部門が該当します。

一般的な項目について

■初めに，機関名とentityIDを記入してください。

Q1.機関名

※必須

Q2.entityID

※必須

不明な場合は，学認申請システムにログインして確認してください

entityIDは通常， "https://idp.nii.ac.jp/idp/shibboleth" のようなURL形式で表されます。

■利用IDの範囲と概数はどれくらいになるか，教職員・学生・その他にわけて，当てはまるものを（差し支えのない範囲で）お答えください。

Q3.教職員のID数

※必須

1. 非公表
2. 教職員には発行していない
3. 500以下
4. 501-1000
5. 1001-5000
6. 5001以上

Q4.学生のID数

※必須

1. 非公表
2. 学生には発行していない
3. 500以下
4. 501-1000
5. 1001-5000
6. 5001-10000
7. 10001以上

Q5.その他のID数（学生・教職員以外のID数をご回答ください。卒業生のIDも含めないでください。）

※必須

1. 非公表
2. 学生・教職員以外には発行していない
3. 500以下
4. 501-1000
5. 1001-5000
6. 5001以上

■本アンケートに回答していただく方(問い合わせ責任者)について記入してください。

Q6.お名前

※必須

Q7.IdP運用上でのご担当 ※必須

参考：学認実施要領（ https://www.gakunin.jp/document/74 ）第10条（運用責任者），第11条（運用担当者）

1. IdP運用責任者
2. IdP運用担当者
3. IDaaSの担当者
4. その他記入担当

その他のテキストを入力してください

利用者IDと属性の管理・運用について

■IdPを運用する上での根拠規則や内規の制定状況について記入してください。

※必要に応じて下記の部門に照会してください。

★ポリシー管理部門

Q8.IdP運用上での根拠規則や内規の制定状況について ※必須

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. 「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。
9. その他

Q8-a.「その他」と答えた場合及び，1または2と回答し公開されているURLがある場合は，具体的に記入してください。

■利用者IDの管理方法について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

▼システム管理部門

★ポリシー管理部門

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？ ※必須

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。
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。
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。
4. その他

その他のテキストを入力してください

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
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

その他のテキストを入力してください

Q11.リリースされる属性は，組織メンバーとそれ以外で区別できるようになっていますか？ ※必須

1. 区別できるようになっている。
2. 区別できるようにはなっていない。

Q12.Q10で，特にゲストアカウントを含む臨時のアカウント等について例外的な運用が認められていますか？ ※必須

1. ゲストアカウント等の作成は規則で禁止されている。
2. ゲストアカウント等の作成は認められており，一元管理されている。
3. ゲストアカウント等の作成は認められており，部局の裁量で作成できる。

Q13.前項（Q12）で「ゲストアカウント等の作成は認められており，一元管理されている。」と答えた場合，その管理体制や運用体制はどう定められていますか？（技術運用基準8.1）

l ゲストアカウントの利用について，作成部局長が責任をとる体制になっており，そのもとでIdP管理者がアカウントを個別に発行することにしている。
l ゲストアカウントの作成は部局の裁量でできるが，IdPは，ゲストアカウントとそれ以外の区別ができる運用になっており，ゲストアカウントは学認参加のSPにアクセスできない方策を採っている。

■学認参加SPに送出する利用者IDの属性で，IdPが保証しているものの範囲について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

Q14.Q9～13を踏まえてご回答ください。IdPが送出する利用者IDの属性は，自組織のものに限ることが保証される運用になっていますか？（技術運用基準3.2）

※必須

Q14回答例：
l 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ので，自組織のものに限られる。
l 他組織の属性は，このIdPでは付与しない運用になっている。

■IdPが学認参加SPに送信する属性の信頼性について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

▼システム管理部門

★ポリシー管理部門

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）

※必須

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。
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。
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。
4. その他

その他のテキストを入力してください

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。）

※必須

保証している属性（参考：https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158166）

「組織が保証している属性」は，現在のIdP設定で送出可能になっている属性と必ずしも一致しません。換言すれば，組織が保証している属性だが，現在それを利用するSPと連携していないので，送出していないというケースが有り得ます。現状の送出可否にかかわらず，組織が保証している属性について○を選択してください。

属性	組織が保証している属性に，○を選択してください。
mail	選択してください
sn	選択してください
o	選択してください
ou	選択してください
givenName	選択してください
displayName	選択してください

eduPersonスキーマより：

※必須

属性	組織が保証している属性に，○を選択してください。
eduPersonAffiliation	選択してください
eduPersonPrincipalName	選択してください
eduPersonEntitlement	選択してください
eduPersonScopedAffiliation	選択してください
eduPersonTargetedID	選択してください

eduMemberスキーマより：

※必須

属性	組織が保証している属性に，○を選択してください。
isMemberOf	選択してください

jaPerson/jaOrganizationスキーマ（GakuNinスキーマ）より：

※必須

属性	組織が保証している属性に，○を選択してください。
jasn	選択してください
jaGivenName	選択してください
jaDisplayName	選択してください
jao	選択してください
jaou	選択してください
gakuninScopedPersonalUniqueCode	選択してください

追加属性（学認技術運用基準 Ver 2.2で追加）： ※必須

属性	組織が保証している属性に，○を選択してください。
eduPersonAssurance	選択してください
eduPersonUniqueId	選択してください
eduPersonOrcid	選択してください

Q16.属性情報は，技術運用基準で定めるものから選択して利用すべきであるとされています。もし，それ以外のものがあれば，学術認証運営委員会に申請することが必要です。学認を利用するときに，これらのことは守られていますか？（技術運用基準3.1） ※必須

1. 守られている
2. 守られていない

■利用者IDのライフサイクル管理について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

Q17.利用者IDのライフサイクル管理，特に停止や廃棄についてどう規定されていますか？（技術運用基準8.1） ※必須

Q17回答例
l 利用者IDのDBは，管理部局である人事または学務において適切に管理されている。IDのライフサイクル管理もその一環として管理されている。
l 利用者が組織を去った場合，担当部局によって失効作業が行われる体制になっている。

■利用者IDの利用状況について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

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） ※必須

1. 機関全体の認証基盤上のIDであり，各種機関内サービスで利用している
2. 学習管理システムやポートフォリオ，ポータルサイトなどの学生向けのサービスで利用している
3. 経理や人事など，機関の運営に関わるシステムで利用している
4. その他（具体的に記入）

その他のテキストを入力してください

5. 該当するものはない

共有IDの禁止について

■IDの再利用について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

★ポリシー管理部門

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）

※必須

1. 再利用は無い
2. 最低24カ月再利用は無い
3. ルールは定めていない
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
5. その他

その他のテキストを入力してください

■Q19の場合を除き，IdPでは，同一IDでのアクセスが同一人物からによることを保証するための方策を講じなければならないとされています。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

▼システム管理部門

★ポリシー管理部門

Q20.特に，IDとクレデンシャルの配付や管理によってこれを保証する方法を記してください。（技術運用基準8.3）

※必須

Q20回答例
l IDとパスワードの配付は，職員証・学生証を用いて本人確認を行った上で，書面で行っている。
l IDとパスワードの配付は，信頼が置ける学内便等を通して行っている。

Q21.IDの共有を防止するために実施しているQ20以外の方策について記してください。（技術運用基準8.3）

※必須

Q21回答例
l IDの共有をしなくても業務に差支えがないようなロールと権限の管理システムをとっている。
l IDの共有がセキュリティの面から望ましくないことの啓蒙活動を行っている。
l 内規でIDの共有禁止を定めている。
l 実施している方策はQ20のみである

■一般にクレデンシャルの質を保証したり，運用に注意を払うことによってパスワードの安全性を高める方法について記入してください。

※必要に応じて下記の部門に照会してください。

★ポリシー管理部門

Q22.パスワードポリシーは定められていますか？

※必須

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。

Q23.前項（Q22）で「パスワードポリシーを定めている」と答えた場合，その内容を教えてください。

Q23回答例
l 一定以上の長さの指定（例えば6文字以上）
l 数字や特殊文字をパスワードに組み込むことの指定
l 有効期限の設定（例えば1年）

Q24.運用に注意を払うことで安全性を高める努力をしていますか？具体的に記入してください。 ※必須

Q24回答例
l 運用において1年1度の棚卸とパスワード再初期化を行うことで実質的に品質を担保している。
l パスワードに関する事故に対しては，優先的に対応するようにしている。
l 特に定めていないが，啓蒙活動を定期的に行っている。

個人情報保護について

■個人情報保護について記入してください。

※必要に応じて下記の部門に照会してください。

▼システム管理部門

★ポリシー管理部門

Q25.IdPから送信される個人情報について，個人情報の保護に関する法律等，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） ※必須

1. 関連する法令その他に従うように運用されている。
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。

Q26.プライバシーについて，具体的に規定はありますか？ ※必須

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。

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） ※必須

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 組み込みの属性リリース同意取得機能を使っている
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
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

Q28.SPによっては，SPの定める属性以外が送られることを拒否するものがあります。それに対応できるようになっていますか？ 対応方法について，具体的に記入してください。 ※必須

Q28回答例
I 属性のリリースについては，IdPの構成変更を注意深く行うことで対応している。

一般的なセキュリティについて

■ログの保存期間について記入してください。

※必要に応じて下記の部門に照会してください。

▼システム管理部門

★ポリシー管理部門

Q29.ログの保存期間は定められていますか？具体的に記入してください。 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8.7） ※必須

Q29回答例
l ログは6ヶ月保存するように内規で決まっている。

■各参加機関は，自らが送信する情報の信頼性や正確性について努力義務を負うことを規定しています。これまでに記述した以外の運用・管理上での規定について記入してください。（技術運用基準8.8）

※必要に応じて下記の部門に照会してください。

★ポリシー管理部門

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？

※必須

1. 定められている。（以下にURLを記入）

その他のテキストを入力してください

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。

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？

※必須

1. 定められている。（以下にURLを記入）

その他のテキストを入力してください

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。

■IdPの設定ファイルの管理について記入してください。

※必要に応じて下記の部門に照会してください。

▼システム管理部門

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？

※必須

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
3. IDaaSに管理を全て委任している
4. 設定ファイルの管理体制は不明である
5. その他

その他のテキストを入力してください

利用者IDおよびクレデンシャルについて

将来，学外の，より信頼度を要求するようなサービスへの接続が視程に入ってくると，IdPの保証度(LoA)は大きな問題になります。以下はそれを見据えて，各参加機関でどのような対応が現時点でなされているかを調査するものです。

■利用者IDの停止や廃棄について記入してください。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

★ポリシー管理部門

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？ ※必須

1. 1年に1度以上の頻度で定期的に実施している。
2. 1年に複数回の頻度で不定期に実施している。
3. 数年に1度だが定期的に実施している。
4. 定期的には実施していないものの，必要に応じて実施している。
5. 実施していない。

Q34.前項（Q33）で設定したタイミングの理由について教えてください。（複数回答可） ※必須

- [ ] 1. 作業漏れを発生させたくない。
- [ ] 2. 遅延を発生させたくない。
- [ ] 3. 作業工数を最小にしたい。
- [ ] 4. その他（具体的に記入）

その他のテキストを入力してください

Q35.Q33の規定状況について教えてください。 ※必須

- [ ] 1. 手続きの内容，タイミングが規程で明文化されている。
- [ ] 2. 手続きの内容のみ明文化されている。
- [ ] 3. 手続きのタイミングのみ明文化されている。
- [ ] 4. いずれも明文化されていないが自主的に実施している。
- [ ] 5. その他（具体的に記入）

その他のテキストを入力してください

Q36.非定期な利用者の異動・退職など，Q33で回答したタイミング以外でも利用者IDを停止・廃棄する手続きを行うことはありますか？ ※必須

- ○ 1. はい
- ○ 2. いいえ

Q37.前項（Q36）の規定状況について教えてください。 ※必須

- ○ 1. 手続きの内容，タイミングが規程で明文化されている。
- ○ 2. 手続きの内容のみ明文化されている。
- ○ 3. 手続きのタイミングのみ明文化されている。
- ○ 4. いずれも明文化されていないが自主的に実施している。
- ○ 5. その他（具体的に記入）

その他のテキストを入力してください

■利用者IDのクレデンシャルについて記入して下さい。

※必要に応じて下記の部門に照会してください。

▲ID基盤管理部門

▼システム管理部門

★ポリシー管理部門

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。） ※必須

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
- ○ 2. 電子証明書
- ○ 3. パスワードベースの多要素認証
- ○ 4. その他のクレデンシャル

Q38-a.補足事項があれば記入してください。

Q39.前項（Q38） で「その他のクレデンシャル」と答えた場合，その内容を具体的に教えてください。

Q40.Q38で回答したクレデンシャルの選定理由について教えてください。（複数回答可） ※必須

- [ ] 1. 安全性の確保
- [ ] 2. 導入コストが低い
- [ ] 3. 運用コストが低い
- [ ] 4. ユーザサポートが楽
- [ ] 5. その他（具体的に記入）

その他のテキストを入力してください

Q41.Q38で回答したクレデンシャルの有効期間について教えてください。 ※必須

同一クレデンシャルでも利用者ID種によって複数の有効期間がある場合，あるいはQ38の補足事項欄で補足したクレデンシャルについて有効期間が異なる場合は，典型的な有効期間について選んでいただいた上で，補足事項欄にて補足してください。

- ○ 1. 1年間未満
- ○ 2. 約1年間
- ○ 3. 約2年間
- ○ 4. 約3年間
- ○ 5. 約4年間
- ○ 6. 約5年間
- ○ 7. 有効期間の設定なし
- ○ 8. その他（具体的に記入）

Q41-a.補足事項があれば記入してください。

Q42.前項（Q41） で「その他」と答えた場合，設定した有効期間を具体的に教えてください。

Q43.Q41で設定した有効期間の理由（あるいは有効期間を設定しない理由）について教えてください。（複数回答可） ※必須

- [ ] 1. 安全性
- [ ] 2. 人事のライフサイクルとの連動
- [ ] 3. 更新コストの最小化
- [ ] 4. その他（具体的に記入）

その他のテキストを入力してください

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について教えてください。（複数回答可）

※必須

- [ ] 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）

その他のテキストを入力してください

- [ ] 10. 該当するものはない

Q45.前項（Q44）をより確実にするために該当する取り組みがあれば教えてください。（複数回答可）

※必須

- [ ] 1. Q44の条件が必須となるようシステムで制約をかけている。
- [ ] 2. Q44の条件を全学の情報セキュリティポリシー等で必須事項として規定している。
- [ ] 3. Q44の条件を全学の情報セキュリティポリシー等で推奨事項として規定している。
- [ ] 4. その他（具体的に記入）

その他のテキストを入力してください

- [ ] 5. 該当するものはない

Q46.クレデンシャル危殆化時の手続き（利用者IDの停止やクレデンシャルの更新など）を行うタイミングについて教えてください。（複数回答可） ※必須

- [ ] 1. 利用者あるいは利用者の所属部局などから申請があれば速やかに対応する。
- [ ] 2. 不正利用など危殆化の疑いがある場合，申請がなくても場合によっては運用部局等の判断で速やかに対応する。
- [ ] 3. その他（具体的に記入）

その他のテキストを入力してください

Q47.前項（Q46）の規定状況について教えてください。 ※必須

- ○ 1. 手続きの内容，タイミングが規程で明文化されている。
- ○ 2. 手続きの内容のみ明文化されている。
- ○ 3. 手続きのタイミングのみ明文化されている。
- ○ 4. いずれも明文化されていないが自主的に実施している。
- ○ 5. その他（具体的に記入）

その他のテキストを入力してください

ソフトウェアのアップデート状況について

■学認事務局からお知らせしたセキュリティアドバイザリへの対応状況について記入してください。

※必要に応じて下記の部門に照会してください。

▼システム管理部門

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2025年9月以降に事務局からお知らせしたものです。 ※必須

注意喚起内容	対応状況
[upki-fed:126] 【注意喚起】Apache HTTP Serverの脆弱性について (CVE-2025-58098) 2026/1/9	選択してください
[upki-fed:128] 【注意喚起】OpenSSLの脆弱性について (2026/1/27付アドバイザリ) 2026/2/5	選択してください
[upki-fed:134] 【注意喚起】Jettyの脆弱性について (2026/03/06付アドバイザリ) 2026/3/30	選択してください
[upki-fed:136] 【注意喚起】Jettyの脆弱性について 2026/4/27	選択してください
[upki-fed:137] 【注意喚起】Java SE JDK及びJREの脆弱性について(2026年4月) 2026/5/7	選択してください
[upki-fed:142] 【注意喚起】Shibboleth IdPの脆弱性について(2026/5/13付アドバイザリ) 2026/5/21	選択してください
[upki-fed:144] 【注意喚起】Apache HTTP Serverの脆弱性について (CVE-2026-28780) 2026/6/10	選択してください
[upki-fed:150] 【注意喚起】Java SE JDK及びJREの脆弱性について(2026年7月) 2026/8/7	選択してください
[upki-fed:151] 【注意喚起】Apache HTTP Serverの脆弱性について (CVE-2026-34355等) 2026/8/7	選択してください
[upki-fed:152] 【注意喚起】Jettyの脆弱性について (CVE-2026-10050等) 2026/8/7	選択してください

■IdPで稼働しているソフトウェアについて教えてください。

※必要に応じて下記の部門に照会してください。

▼システム管理部門

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 4.x系は2024年9月1日でサポートが終了しました。) 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） ※必須

1. Shibboleth IdP 5.x系統にアップグレード済みである
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
3. 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（来年度以降のアップグレード予定を含む）
4. 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
5. 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）
6. Shibboleth IdP以外のソフトウェアでIdPを運用している
7. 稼働しているソフトウェアは不明である
8. アプライアンス製品を利用してIdPを運用している
9. 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
10. その他（具体的に記入）

Q49-a.6と答えた場合は，ソフトウェア名を記載の上，そのバージョンを2行目に記入してください。 10と答えた場合は，具体的にご記入ください。

Q49-b.8または9と答えた場合，よろしければ利用されている製品名・サービス名を記入してください。また，その製品・サービスが使用しているソフトウェアを把握している場合はそのソフトウェア名を2行目に追記し，さらに，そのバージョンを把握している場合は3行目に追記し，加えてShibboleth IdPの場合はQ49の選択肢1～5から番号を追記してください。

運用責任者の職責について

■2023年4月の学認実施要領の改定に伴う，貴機関の運用責任者の職責について記入してください。

※必要に応じて下記の部門に照会してください。

●IdP運用担当部門

Q50.学認実施要領は2023年4月に改定されております。改定後，運用責任者は「IdPの管理・運用を担う部門の長など機関・組織としての責任を負える者であること」と規定されておりますが，貴機関の運用責任者はこちらの要件を満たしているか，教えてください。なお，規程中「機関・組織」とされておりますが，後者は機関の組織として学認に参加した方向けの文言ですので，そうでない方は「機関」と解釈してお答えください。(実施要領10) ※必須

学認実施要領 2023年4月改定 https://www.gakunin.jp/news/20230330

1. 改定内容を承知しており、要件を満たしている
2. 改定内容を承知しているが、要件を満たしていない
3. 改定内容を承知していなかったが、現状で要件を満たしている
4. 改定内容を承知しておらず、要件を満たしていない

メタデータ記載証明書の更新状況について

■メタデータに記載している証明書について記入してください。

※必要に応じて下記の部門に照会してください。

●IdP運用担当部門

▼システム管理部門

Q51.IdPがXML署名等を行う，学認に登録しメタデータに記載されている証明書は，「3年を目処に定期的に更新すべきである」と規定されております。当該証明書の更新状況について教えてください。（技術運用基準7.4） ※必須

1. 有効期限内に更新している
2. 発行後3年以内に更新している
3. 3年を超えるが定期的に更新している
4. 更新していない
5. 不明である

ご回答ありがとうございました

回答必須の設問は以上です。よろしければ，次の設問にもご回答ください。

※必須ではございません。

Q52.MFA（多要素認証）・Passkey等の認証方式について，貴機関における導入・利用の状況を教えてください。

具体的には，導入済みの認証方式，対象となっている利用者・システム，導入・利用を進める上での課題，今後の導入・拡大の予定などについて，差し支えない範囲でご回答ください。

Q53.その他お気づきの点がありましたら，ご自由にお書きください。

IdPサーバの管理運用で苦労されていること，次世代認証連携などの学認を取り巻くトピックで気になっていることなど，ご意見ご要望などいただけますと幸いでございます。

参考：次世代認証連携の取り組み　https://www.gakunin.jp/fed/ng