1ページ目（1/6）：　一般的な項目について

学認アンケートにご協力いただきましてありがとうございます。
アンケートは全部で6ページです。

＊マークのある質問は回答必須です。

Q1～2：
初めに，機関名とentityIDを記入してください。

＊ 1. 機関名

＊ 2. entityID

Q3～5：
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。

3. 教職員のID数について（差し支えのない範囲で）お答えください。

- ○ 非公表
- ○ 教職員には発行していない
- ○ 500以下
- ○ 501-1000
- ○ 1001-5000
- ○ 5000以上

4. 学生のID数について（差し支えのない範囲で）お答えください。

- ○ 非公表
- ○ 学生には発行していない
- ○ 500以下
- ○ 501-1000
- ○ 1001-5000
- ○ 5001-10000
- ○ 10000以上

5. その他のID数について（差し支えのない範囲で）お答えください。

○ 非公表

○ 教職員と学生以外には発行していない

○ 500以下

○ 501-1000

○ 1001-5000

○ 5000以上

Q6~7：
本アンケートに回答していただく方について記入してください。

* 6. お名前

* 7. IdP運用上でのご担当

○ IdP運用責任者

○ IdP運用担当者

○ その他記入担当

Q8：
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定められていれば記入してください。

8. IdP運用上での根拠規則や内規の制定状況について

Q8 回答例：

- 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 】
- 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 】
- 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。
- 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。
- 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。
- 規則などは特にないが，現在制定中である。
- 全学的にはテスト利用の扱いになっている。

2ページ目（2/6）：　利用者IDと属性の管理・運用について

Q9~13：
利用者IDの管理方法について記入してください。

9. 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（Trusted DB）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。

○ 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

○ 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

○ 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

○ その他

10. 前項（Q9）で，学務データや人事データ等，組織のメンバーを規定する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。

Q10 回答例：

- 卒業生や地域交流センター職員，関連財団職員，図書館の地域内利用者を含む臨時利用者にもIDを与えている。これらには，職位(eduPersonAffiliation/eduPersonScopedAffiliation)としてstaff, student, faculty, member属性がつかない運用をしている。
- 人事データのTrusted DBには存在しないが，大学の業務遂行上必要な者にかぎり，利用者IDを与えている。
- 本学セキュリティポリシー及び関連規程に基づき，利用者IDを作成している。
- 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。

11. 組織メンバーとそれ以外で，リリースされる属性上，両者の区別はできるようになっていますか？

○ 区別できるようになっている

○ 区別できるようにはなっていない

12. 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？

○ ゲストアカウント等の作成は規則で禁止されている

○ 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

○ 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

13. 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）

Q13 回答例：

- 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。
- 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。

Q14：
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。

14. Q9~13 によって，利用者IDの属性で，IdPが保証しているものは，自組織のものに限ることが保証されている運用になっていますか？（技術運用基準3.2）

Q14 回答例：

- 利用者IDの属性は，Trusted DBの属性のみから計算されている。
- 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。

Q15：
IdPが送信する属性の信頼性について記入してください。

15. 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）

また，属性について，組織が保証しているもの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。）

Q15 回答例：

- 利用者IDの属性は，静的にIdPで決定できるもの（organizationNameおよびjaOrganizationName）以外はTrusted DBの属性のみから計算されている。また，特にわれわれが保証しているものは以下の属性である。
  - o (大学名で固定されている。要求するところにはリリース可)
  - ou (所属部局名が必須で入る。要求するところにはリリース可)
  - eduPersonAffiliation (メンバーの身分が入る。要求するところにはリリース可)
  - eduPersonScopedAffliation (メンバーの身分が入る。要求するところにはリリース可)

Q16：
属性情報においての技術運用基準の順守について記入してください。

16. 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）

○ 守られている

○ 守られていない

Q17：
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。

17. 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）

Q17 回答例：

- 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。
- 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。

3ページ目（3/6）：　共有IDの禁止について

Q18：
IDの再利用について記入してください。

18. 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）

Q18 回答例：

- eduPersonPrincipalNameについては，最低24ヶ月間は再利用されることがないような生成規則を取っている。

eduPersonTargetedIDについては，最低24ヶ月間再利用されないことをIdPが保証している。

- 再利用はない。
- 両属性の送出が必要となるサービスは利用していない。また，今後の利用予定もない。

Q19～23：
Q18 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。

19. 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）

Q19 回答例：

- 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。
- 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。

20. IDの共有を防止するためにQ19 以外の方策を実施している場合，それを記してください。（技術運用基準8.3）

Q20 回答例：

- 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。
- 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。
- 内規でIDの共有禁止を定めている。

Q21～23：
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を定めていれば書いてください。

21. パスワードポリシーは定められていますか？

○ パスワードポリシーを定めている。

○ 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。

○ 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。

22. 前項（Q21）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。

Q22 回答例：

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

23. 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？

Q23 回答例：

- 運用において1年一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。
- 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。
- 特に定めていないが，啓蒙活動を定期的に行っている。

4ページ目（4/6）：　個人情報保護について

Q24～27：
個人情報保護について記入してください。

24. 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）

- ○ 関連する法令その他に従うように運用されている
- ○ 関連する法令その他に従うようには運用されていない

25. プライバシーについて，具体的に規定はありますか？

- ○ プライバシーについての具体的な規定がある
- ○ 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
- ○ プライバシーについての具体的な規定はない

26. 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）

- ○ uApprove もしくはその派生版を利用している
- ○ uApprove およびその派生版は利用していない

27. 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？

Q27 回答例：

- 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。

5ページ目（5/6）：　一般的なセキュリティについて

Q28：
ログの保存期間について記入してください。

28. ログの保存期間は定められていますか？
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）

Q28 回答例：
- ログは6ヶ月保存するように内規で決まっている。

Q29～30：
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に，運用・管理上での規定があれば記入してください。（技術運用基準8.8）

29. 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？

○ 定められている（以下にURLを記入）

○ 定められているが，学内限定公開の扱いである

○ 特に定められていない

定められている場合のURL

30. 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？

○ 定められている（以下にURLを記入）

○ 定められているが，学内限定公開の扱いである

○ 特に定められていない

定められている場合のURL

6ページ目（6/6）：　（任意）利用者IDおよびクレデンシャルについて

以下についての回答は完全任意です。

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，各研究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。

なお，組織を特定しない形での統計情報を公開する以外には，回答を公開したり，回答の有無，内容による不利な扱いをしたりすることはありません。

Q31～35：
利用者IDの停止や廃棄について，差し支えなければ記入して下さい。

31. 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？

- ○ 1年に1度以上の頻度で定期的に実施している
- ○ 数年に1度だが定期的に実施している
- ○ 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
- ○ 実施していない

32. 前項（Q31）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）

- ☐ 作業漏れを発生させたくないから
- ☐ 遅延を発生させたくないから
- ☐ 作業工数を最小にしたいから

その他

33. Q31 の規定状況について教えてください。

- ○ 手続きの内容，タイミングが規程で明文化されている。
- ○ 手続きの内容のみ明文化されている。
- ○ 手続きのタイミングのみ明文化されている。
- ○ いずれも明文化されていないが自主的に実施している。

その他

34. 非定期な利用者の異動・退職など，Q31 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？

○ はい

○ いいえ

35. 前項（Q34）の規定状況について教えてください。

○ 手続きの内容，タイミングが規程で明文化されている

○ 手続きの内容のみ明文化されている

○ 手続きのタイミングのみ明文化されている

○ いずれも明文化されていないが自主的に実施している

その他

Q36～43：
利用者IDのクレデンシャルについて，差し支えなければ記入して下さい。

36. 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。

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。

○ パスワード

○ 電子証明書

○ パスワードベースの多要素認証

○ その他のクレデンシャル

補足事項

37. 前項（Q36） 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。

以下，クレデンシャルにまつわる質問をいくつか用意していますが，いずれも Q36 で回答した主要なクレデンシャルを対象とした質問という位置付けでご回答ください。

38. Q36 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）

☐ 安全性の確保

☐ 導入コストが低い

☐ 運用コストが低い

☐ ユーザサポートが楽

その他

39. Q36 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。

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 Q36 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，補足事項にて補足してください。

○ 1年間未満

○ 約1年間

○ 約2年間

○ 約3年間

○ 約4年間

○ 約5年間

○ その他

補足事項

40. 前項（Q39） 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。

41. Q39 で設定した有効期間の理由について教えてください。（複数回答可）

☐ 安全性

☐ 人事のライフサイクルとの連動

☐ 更新コストの最小化

その他

42. 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）

☐ パスワードを8文字以上となるように推奨している

☐ 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

☐ 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

☐ 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

その他

43. 前項（Q42）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）

☐ Q42 の条件が必須となるようシステムで制約をかけている

☐ Q42 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

☐ Q42 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

その他

44. 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）

☐ 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

☐ 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

その他

45. 前項（Q44）の規定状況について教えてください。

○ 手続きの内容，タイミングが規程で明文化されている

○ 手続きの内容のみ明文化されている

○ 手続きのタイミングのみ明文化されている

○ いずれも明文化されていないが自主的に実施している

その他