Q1. 一般的な項目について

Q1-1. 機関名を記入してください。

Q1-2. entityID を記入してください。

Q1-3. 利用ＩＤの範囲と概数はどれくらいになるか、差し支えのない範囲でお答えください。

回答例

1. 全学、利用ＩＤは約 10,000
2. 全学、利用ＩＤは約 10,000（教職員 3,000、学生 7,000）
3. 全学、利用ＩＤは非公表でお願いします。

Q1-4. 以下の項目に回答していただく方のお名前を記入してください。

回答例

1. IdP 運用担当者　○○　○○
2. IdP 運用責任者　○○　○○（記入担当　○○　○○）

Q1-5. IdP を運用する上での根拠規則や内規が定められていれば記入してください。

回答例

1. 全学情報サービス担当の情報基盤センターの内規として以下がある。
   IdP 運用規則　全学サービスセキュリティポリシー（以下の URL から入手可能 http://○○○○）
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が、学内限定で公開されている。
3. 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。
4. 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。
5. 全学的にはテスト利用の扱いになっている。

Q2. 利用者ＩＤと属性の管理・運用について

Q2-1. 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？
回答例

1. 利用者ＩＤのデータベースは一元管理されている[人事部所管と学務部所管の]組織にとってTrusted DBから直接データを送信して作られている。
2. 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行っている。

Q2-2. 上記で、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の他から利用者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。また、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？
回答例

1. 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、eduPersonAffiliationとしてstaff, student, faculty属性がつかない運用をしている。
2. 派遣職員は、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であると考え、利用者ＩＤを与えている。

Q2-3. 上記で、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る場合、その管理体制や運用体制はどう定められていますか？
回答例

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. ゲストアカウントは、部局の裁量でできるという意味で一元管理されていないが、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。
3. 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GakuNin参加のSPにアクセスできない方策を採っている。

Q2-4. Q2-1～3 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？
回答例

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. 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。

Q2-5. 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、Q2-1. によって自動的に生成されるようになっていますか？
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。）
回答例

1. 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。
    1. 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）
    2. 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）
    3. 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）
    4. 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）

Q2-6. 属性情報は、システム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、認証作業部会に申請することが必要です。GakuNin を利用するときに、これらのことは守られていますか？
回答例

1. IdP がリリースする属性は、システム運用基準で定めるものである。

Q2-7. 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？
回答例

1. 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。
2. 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。

Q3. 共有ＩＤの禁止について
Q3-1. eduPersonPrincipalName と eduPersonTargettedID 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？
回答例

1. 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。eduPersonTargettedID 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。

Q3-2. Q3-1 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。
Q3-2-1. 特に、ID とクレデンシャルの配布や管理によってこれを保証する方法を記してください。
回答例

1. ＩＤとパスワードの配布は、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。
2. ＩＤとパスワードの配布は、信頼が置ける学内便等を通して行っている。

Q3-2-2. ＩＤの共有を防止するために Q3-2-1 以外の方策を実施している場合、それを記してください。

回答例

1. 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。
2. 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。

Q3-2-3. 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。
Q3-2-3-1. パスワードポリシーは定められていますか？
回答例

1. 以下に関するパスワードポリシーを定めている。
    1. 一定以上の長さの指定（例えば６文字以上）
    2. 数字や特殊文字をパスワードに組み込むことの指定
    3. 有効期限の設定（例えば１年）
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。

Q3-2-3-2. 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？
回答例

1. 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。
2. 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。
3. 特に定めていないが、啓蒙活動を定期的に行っている。

Q4. 個人情報保護について
Q4-1. 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？具体的に規定はありますか？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。それにも対応できるようになっていますか？
回答例

1. 学内外にプライバシーポリシーを開示している。IdP の運用に際し、プ ライバシーについての具体的な規程はないが､利用者ＩＤとその属性は安全に運用されている。新たなＳＰのサービスを利用するときの属性リリースに際しては uApprove を運用している。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。
2. 学内外にプライバ シーポリシーを開示している。IdP の運用に際し、プライバシーについての具体的な規程はないが､利用者ＩＤとその属性は安全に運用されている。新たな SP のサービスを利用するときには、書面またはオンラインで利用者許諾を得ないと利用できないように運用している。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。

Q5. 一般的なセキュリティについて

Q5-1. ログの保存期間は定められていますか？システム運用基準では推奨項目になっています。

回答例

1. ログは 6 ヶ月保存するように内規で決まっている。

Q5-2. 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してください。

Q5-2-1. 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？

回答例

1. 定められている。http://○○○○で公開している。
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。

Q5-2-2. 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？

回答例

1. 定められている。http://〇〇〇〇で公開している。
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。