2021-10-20

学認次世代認証連携検討作業部会

CrP/CrPS の例の提示（案）

別文書における 1.1 の場合と 1.2 の場合それぞれについて CrP/CrPS の一例を提示する。さらに IDaaS が IAL2 相当の身元確認を行う場合の CrP/CrPS についても 1.2 の一部として例示する。

以下、Trusted DB に直接接続されるアカウントのみ扱う場合。

クレデンシャルポリシー CrP

1. 本文書について

本文書は、〇〇大学で運用する IdP のクレデンシャルポリシーについて述べる

1.1 IdP の URL は〇〇で、以下の RP に対して認証アサーションを発行する。

A. 本学内のサービス

B. 学認

C. 本学が認めた全国共同利用機関の運用するサービス

D. その他、本学が特に認めたサービス

1.2 本文書の Document ID は取得しない。

2. 本文書のスコープ

本文書は、1.1.B と 1.1.C に参加するサービス提供者に認証アサーションを提供する際に、身元確認保証レベルを判断するための情報を提供する

3. 本文書の対象のアカウント

3.1 アカウント

本文書では、本学が提供する全学共通 ID に対する身元確認保証レベルを対象とする

3.2 アカウントに結合されている属性

3.1 で定めるアカウントに結合する属性のうち、以下についてはその保証レベルを身元確認保証レベルと同一に運用する。

A. Organization (〇〇)

B. CommonName

C. eduPersonPrincipalName

D. eduPersonAffiliation (student/staff/faculty)

E. mail

上記のうち、eduPersonPrincipalName は、本学の全学共通 ID と一致することを保証する。

4. アカウントの身元確認の方法

IdP は、本学の学務システムで運用されている本学学生情報又は人事システムで運用されている本学教職員情報から直接情報を得て、アカウントを生成する。

4.1 各方法が適用できる利用者の範囲

A. 利用者アカウントのうち、eduPersonAffiliation として student 属性を持つものは、学務システムの登録手続きに従っていることを保証する。

B. 利用者アカウントのうち、eduPersonAffiliation として staff または faculty 属性を持つものは、人事システムの登録手続きに従っていることを保証する。

クレデンシャルポリシー実施要領 CrPS

1. 本文書について

本文書は、IdP の CrP の具体的な実施要領について定める。

2. 本文書のスコープ

本文書は、アカウントの生成の際の身元確認の具体的な方法について述べる。

3. アカウントの身元確認の具体的な方法

A. 学務システムへの登録は、入学志願から始まる本学の入学手続きの結果行われる。その実際は、本学の関連する内規、および文部科学省の指導に従う。

B. 人事システムへの登録は、本学の教職員採用手続きの結果行われる。その実際は、本学の関連する内規に従う。

3.1 身元確認が不成功だった場合の対処方法

身元確認に成功せず、学務システム又は人事システムからアカウント情報を得られない場合、IdP は、当該人について、いかなる場合でもアカウントを作成しない。

4. プライバシーへの配慮

A. IdP は、個人情報の扱いについては最小限の原則に従って運用する。

B. IdP は、属性の利用方法について、利用者にあらかじめ通知する。特に、学外のサービス提供者に属性を提供する場合は、同意プロセスを利用者に提供する。

5. セキュリティ対策

IdP は、セキュリティ対策に万全の対策を講じる。

6. サービス終了時の手続き

IdP がサービスを終了する場合、保持している個人情報は、後日のアクセスを可能にしないように完全に廃棄破壊する。

以下、自ら利用者情報を収集してアカウントを作成し、サービスを行う場合。共同利用機関が自ら IdP を運用する場合、または IDaaS が、既存のトラストに属しない組織又は個人に対してアカウントを発行する場合

クレデンシャルポリシー CrP

1. 本文書について

本文書は、〇〇研究所で運用する共同利用サービスのための IdP のクレデンシャルポリシーについて述べる

1.1 IdP の URL は〇〇で、以下の RP に対して認証アサーションを発行する。

A. 本研究所内のサービス

B. 学認

C. 本研究所が全国共同利用機関としてサービスに供するためのアイデンティティサービス

D. その他、本研究所が特に認めたサービス

1.2 本文書の Document ID は取得しない。

2. 本文書のスコープ

本文書は、1.1.C に参加するサービス提供者に認証アサーションを提供する際に、身元確認保証レベルを判断するための情報を提供する

3. 本文書の対象のアカウント

3.1 アカウント

本文書では、本研究所が提供するアカウント全体に対する身元確認保証レベルを対象とする

3.2 アカウントに結合されている属性

3.1 で定めるアカウントに結合する属性のうち、以下についてはその保証レベルを身元確認保証レベルと同一に運用する。

A. Organization。ただし、OU 属性として Others が与えられているものを除く。

B. CommonName

C. eduPersonPrincipalName

D. eduPersonAffiliation

E. mail

4. アカウントの身元確認の方法

IdP は、本学の学務システムで運用されている本学学生情報又は人事システムで運用されている本学教職員情報から直接情報を得て、アカウントを生成する。また、本研究所に属しない人間に対してもアカウントを発行することがある。

4.1 各方法が適用できる利用者の範囲

A. 利用者アカウントのうち、eduPersonAffiliation として student 属性を持つものは、本研究所と提携し、学認に属する大学の学務システムの登録手続きに従っていることを保証する。

B. 利用者アカウントのうち、eduPersonAffiliation として staff または faculty 属性を持つものは、人事システムの登録手続きに従っていることを保証する。

C. 本研究所に属しない人間に対して発行するアカウントに対しては、eduPersonAffiliation として member 属性を発行する。本研究所の学務システム又は人事システムに登録されていないものに対応し、5.で定める方法を適用する

5. 本研究所に属しない人間に対するアカウント発行について

A. 本研究所が規定する証拠の提出、必要に応じて当研究所の指定する職員のエンドース書類の提出を求める。

B. 実在性確認のために、以下のうちいずれかを実施する

a. 指定された係員による対面での面接

b. 十分な通信画質品質を保証した上でのリモート面接。この場合、必要に応じて、監査のために、録画を面接記録として保持する。

c. a., b. を伴わない書類審査のみで、実在性確認をすることはない

C. アドレス確認のための手続きを定め、運用する。

a. 証拠に記された住所を信頼する

b. 携帯電話の番号確認は、対面、又はリモートでの面接での架電で行う

c. 固定電話の番号確認は、所属組織の代表番号への架電を経て行う。

d. 電子メールアドレスは、身元確認の手続き中には信頼できるものとしては扱わない。

クレデンシャルポリシー実施要領 CrPS

1. 本文書について

本文書は、IdP の CrP の具体的な実施要領について定める。

2. 本文書のスコープ

本文書は、アカウントの生成の際の身元確認の具体的な方法について述べる。

3. アカウントの身元確認の具体的な方法

A. eduPersonAffiliation として student 属性を発行する場合、本研究所と提携し、学認に属する大学の学務システムへの登録が、入学志願から始まる本学の入学手続きの結果行われることを、当該大学と学認から提供される資料を元に判断する。

B. edupersonAffliliation として staff 又は faculty を発行する場合、本研究所の人事システムへの登録は、本研究所の教職員採用手続きの結果行われる。その実際は、本研究所の関連する内規に従う。

C. 本研究所に属しない人間の身元確認として、以下を実施する。

a.身元確認に際し、申請者に対して以下の証拠の提出を求める

1. パスポート、免許証、マイナンバーカード等、公的機関が発行した写真付き身分証明書の写し 2 通　又は

2. 公的機関が発行した写真付き身分証明書の写し 1 通と、本研究所が指定した 2 人以上の研究所職員によるそれぞれのエンドース書類 2 通 又は

3. 学認に属する研究機関で IAL2 の認定を受けたものについてはその AAL2 以上での認証を行ったアサーション 1 通。その中で発行した IdP が IAL2 以上を保証した属性値を認める。又は

4. 自分の属する会社の写真付き社員証を提出しても良い。身元確認の審査に際して、一定の証明力を認めることがある。

5. 提出された証拠は、提出人の一意性を担保するために、定められた期間保存し、過去に同一申請人が申請したかどうかの判断に用いることがある。

6. 審査の結果作られたアカウントは、一定の期間後、又は当人の社会的状態が変化したと本研究所が判断した時点で無効化され、再度審査の上アカウントが与えられる。無効化されたアカウントとの連続性は保証しない。

7. 提出された証拠は、申請人の一意性を確認するために、必要なセキュリティ上の措置を講じて本研究所内に保存する。対象となるアカウントが削除された場合、証拠は削除される。

b. 提出された証拠の妥当性確認は、本研究所の指定された職員によって行う。職員の職位はあらかじめ公開する。

c. 証拠の検証は、対面又はリモートでの面接時に、証拠に提示されている写真と本人の一致の確認を含む手続きを経て行う。

3.1 身元確認が不成功だった場合の対処方法

A. 本研究所に属する職員、又は提携する大学の学生について身元確認が成功しなかった場合、IdP は、いかなる場合においても当該人のアカウントを作成しない。

B. 本研究所に属しない人間の身元確認に成功しなかった場合、2 週間以内に本研究所の指定する苦情処理委員会に申し立てがなされた場合、身元確認の妥当性を審査し、結果を当該人に通知する。申し立ては、連続する 6 か月内に 2 度以上は受理しない。

4. プライバシーへの配慮

A.　IdP は、個人情報の扱いについては最小限の原則に従って運用する。

B.　IdP は、属性の利用方法について、利用者にあらかじめ通知する。特に、学外のサービス提供者に属性を提供する場合は、同意プロセスを利用者に提供する。

5. セキュリティ対策

IdP は、セキュリティ対策に万全の対策を講じる。

6. 記録

身元確認のために行った手続きはすべて記録し、別に定めのある場合を除いてサービス終了まで保持する。

7. サービス終了時の手続き

IdP がサービスを終了する場合、保持している個人情報は、後日のアクセスを可能にしないように完全に廃棄破壊する。