C2601 全学認証基盤運用管理規程

国立情報学研究所 学術情報ネットワーク運営・連携本部  
高等教育機関における情報セキュリティポリシー推進部会

**改定履歴**

|  |  |  |
| --- | --- | --- |
| 日付・文書番号 | 改定内容 | 担当 |
| 2016年2月5日  C2601 | 新規作成 | 曽根秀昭（東北大学、高等教育機関における情報セキュリティポリシー推進部会主査）  岡部寿男（京都大学）  佐藤周行（東京大学）  野田英明（国立情報学研究所） |

本文書の内容についてのご質問、ご意見は以下まで電子メールにてお寄せください。

sp-comment[at]nii.ac.jp　（[at]を＠に置き換えてください）

担当者の所属は改定当時のものです。担当者への直接のご質問はご遠慮ください。

C2601-01（目的）

第一条　この規程は、A大学全学認証基盤（以下「本基盤」という。）の運用及び管理に必要な事項を定め、もってシステムの安定的・円滑な運用を維持することを目的とする。

備考：　この規程は全学認証基盤（システム）を扱い、他のシステムとの認証接続についてはC2602 全学認証基盤認証接続規程、全学アカウントについてはC2603 全学認証基盤アカウント利用規程で定める

C2601-02（定義）

第二条　この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　A大学全学認証基盤　A大学における教育研究、福利厚生のためのサービスを提供する際に必要となる、利用者認証と主体認証情報の提供を行う情報システムをいう。

二　利用者　本基盤のアカウントの発行を受けることができる者をいう。

三　識別コード 本基盤及び本基盤より機能の提供を受ける情報システムにおいて用いる、利用者を一意に識別するための符号をいう。

四　主体認証情報　識別コードを提示した利用者が本人であることを確認するための秘密情報等をいう。

五　全学アカウント　本基盤で主体認証を行う情報システムにおいて、主体に付与された正当な権限をいう。全学アカウントの付与は、識別コードと主体認証情報の配布、主体認証情報格納装置の交付、アクセス制御における許可、またはそれらの組み合わせ等によって行われる。

五　属性情報　全学アカウントに付随して管理・提供される利用者に関する情報をいう。

六　アイデンティティ情報　利用者に関する全学アカウントおよび属性情報を総称する情報をいう。

七　認証接続　認証と認可を目的として、全学情報システム、もしくは部局情報システムが本基盤のアイデンティティ情報を利用することをいう。

備考：　部局情報システムには部局が契約する学外の情報サービスのシステムも含まれる。学外の情報サービスのシステムとの認証接続にはいずれかの部局の契約を必須とするので、学外の情報システムとの認証接続は存在しない。

八　認証接続システム　本基盤に認証接続された全学情報システムもしくは部局情報システムをいう。

九　認証接続責任者　認証接続システムの認証接続に係る責任を有する本学の職員をいう。

十　A大学認証局　A大学電子認証局ポリシー及び運用規則に定める認証局をいう。

十一 電子証明書 A大学認証局から発行された証明書でログイン時の主体認証等に利用するため証明書をいう。

十二 ICカード C2101-02情報システム運用・管理規程第二条三十八に定める主体認証情報格納装置のうち、主体認証情報をICに格納するものをいう

十三 PIN (Personal Identification Number) 電子証明書を格納したICカードを使った主体認証時に使われる主体認証情報をいう。

備考：　認証接続システムの部局技術責任者が認証接続責任者となる。

C2601-03（運用責任者）

第三条　本基盤の運用責任者（以下「運用責任者」という。）は全学実施責任者をもって充てる。

C2601-04（認証情報）

第四条　運用責任者は、本基盤において利用する主体認証情報について、パスワードを用いる場合には、別途定める利用者パスワードガイドラインに基づき、利用者に認証強度が一定以上のものを利用させるよう配慮するものとする。

備考：　C3255利用者パスワードガイドラインがある。

C2601-05（属性情報）

第五条　本基盤が保有する利用者の属性情報の項目は運用責任者が別に定める。

２　本基盤が保有する利用者の属性情報のうち職員データベースおよび学生データベース（以下、総称してデータベース等という。）から転送されるものについて、それぞれ職員データベース運用管理規程および学生データベース運用管理規程に合致するものでなければならない。

３　運用責任者は、本基盤で登録する属性情報が真正であることを確保するため、必要な措置を講じなければならない。また、利用者または運用責任者が本基盤で更新登録する属性情報を最新の状況を反映させて適切に管理しなければならない。

４　運用責任者は、データベース等から転送された属性情報について、データベース等において更新があった場合にそれを本基盤へ転送しなければならない。

５　運用責任者は、データベース等から転送された属性情報について、利用者または運用責任者が本基盤で更新した属性情報をデータベース等へ反映させるよう適切に管理しなければならない。

６　認証接続システムの利用者または認証接続システムの認証接続責任者が設定して本基盤へ転送する属性情報は、当該認証接続システムの運用管理規定に合致するものでなければならない。

備考：認証基盤が保有する個人情報の登録・削除等の管理について、（ａ）源泉となる個人情報データベースを別に設けて転送（インポート）する、（ｂ）この認証基盤において（源泉として）行う、（ｃ）職員データベースや学生データベースなど既存のデータベース等から転送し、いずれのデータベースにも含まれない者をこの認証基盤において追加する、などの方法が考えられるが、この条では（ｃ）を想定している。  
なお、５は認証基盤で属性情報の更新登録を可能とする場合に源泉となるデータベース等へ反映させることを、６は認証接続システムで属性情報の設定を可能とする場合に認証基盤へ反映させることを定めるものであるので、これらの機能を許さないシステムでは不要である。

C2601-06（認証接続）

第六条　本基盤と認証接続システムの認証接続に関することはA大学全学認証基盤認証接続規程に定める。

C2601-07（全学アカウント）

第七条　全学アカウントに関することは全学認証基盤アカウント利用規程に定める。

C2601-08（個人情報の取り扱い）

第八条　本基盤における個人情報の取扱いは、A大学個人情報保護規程（以下、「個人情報保護規程」という。）の定めるところによる。

２　本基盤の保有個人データについて、本人からの開示、訂正、追加、削除及びその他の個人情報に関する問い合わせは運用責任者が別に定める。

備考：個人情報保護規程は，国立大学等であれば独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）に沿ったものである。  
本基盤において個人情報を取得し、保有および利用することができるのは、次の各号に掲げる目的に必要な場合に限られる。  
　一 A大学全学アカウント付与  
　二 A大学全学認証基盤の維持管理  
　三 認証接続システムとの情報連携サービス  
　四 インシデント対応に不可欠な範囲での利用  
　五 その他運用責任者が必要と定める事項

C2601-09（運用環境）

第九条　本基盤は、物理環境的およびセキュリティ的に適切な環境に設置し、運用責任者は限定された運用管理者を指名してその任に当たらせるものとする。

２　本基盤は、C2101 情報システム運用・管理規程に定める情報セキュリティ基準に準拠して運用するものとする。

３　運用責任者は必要に応じて運用管理者に研修等を定期的に受けさせるものとする。

C2601-10（記録）

第十条　本基盤を用いた利用者の認証について、トランザクションごとに、時刻を認証接続サービスに渡されたアイデンティティ情報等のログ情報とともに記録するものとする。

２　本基盤は、本学が信頼する時刻情報を用いて時刻同期を取るものとする。

３　運用責任者は、ログ情報の保存期間を最低3か月の範囲で定めるものとする。運用管理者は、当該保存期間が満了する日までログ情報の記録を適切に保護された状態で保存し、保存期間を延長する必要がない場合は速やかにこれを消去するものとする。

４　運用責任者は、収集、保管されるログ情報の種類については、定期的にリスク評価を行い、見直すものとする。

C2601-11（雑則）

第十一条　この規程に定めるもののほか、本基盤の運用及び管理に関し必要な事項は、運用責任者が別に定める。