　　　20XX年　　X月　　X日

東海国立大学機構情報連携統括本部長　殿

　　　　　　　　所属長　　役職

氏名　　　　　　　　　　　　〔公印省略〕

【東海国立大学機構】機構統合認証サービス利用申請書

東海国立大学機構統合認証サービス利用内規に基づき，下記の通り申請いたします。

　利用に際しては，利用内規を遵守し，個人情報の保護を徹底する他，利用に当たって問題が生じた場合には貴本部に速やかに報告いたします。

記

1. 希望利用開始年月日：20XX年　　X月　　X日

新規サービスは登録の可否を機構情報戦略室会議（月1~2回）で審議するため、登録作業と合わせて1ヵ月程度を見込む場合があります。申請は余裕をもってご準備ください。  
機構統合認証サービスを利用して提供するサービスの名称及び概要

|  |
| --- |
| サービスの名称  概要： |

1. 責任者

責任者は東海国立大学機構統合認証サービス利用内規，および「本申請内容」を熟知しているものとする。また次の内容について承諾するものとする。

〇提供される統合認証個人情報の利用は，申請されたサーバおよび当該サービスの提供に必要なコンピュータにおいてのみである。

〇情報セキュリティ監査に対応可能である。

* 1. 氏名　　　　　　　　　　　　　　　　　　　②所属

③ 役職 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ※責任者は原則係長級以上の常勤職員、または常勤教員である必要があります

④ 連絡先 電話番号 　　　　　　　　　　　　 E-mail

1. 担当者

担当者は，申請したサービスについて情報連携統括本部からの問い合わせに対応可能であること。

* 1. 氏名　　　　　　　　　　　　　　　　　　　②所属

1. 連絡先 電話番号 　　　　　　　　　　　　 E-mail
2. サービスの問い合わせ先

サービスの問い合わせ先は，エンドユーザーからの問い合わせに対応可能であること。

* + 1. 担当者または担当部署
    2. 電話番号 　　　　　　　　　　　　 E-mail 　　　　　　　　　　　　　　　　 （どちらか必須）
    3. 上記問い合わせ先が，自サービスの画面に □記載がある，または記載予定である ／ □記載しない

「記載しない」を選択の場合は理由をご記入ください。　※本申請が承認されない場合があります

（記入例：テスト運用のため公開されないシステム）

1. サービス監査のための情報

サービス提供予定人数　　　　　　　 人

サービス対象部局：　全学・自部局・自部局の一部（　　　　　　　　）・他部局（　　　　　　　　）

サービス対象者：　学生・役員・教員・事務職員・技術職員・非常勤教員・非常勤職員

研究生・その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　 ）

アクセス公開範囲： 学内・学外・その他（　　　　　　　　　　　　　　　　　　　　　　　　　　）

サービスのURL

サービスを稼働するサーバの情報  
IPアドレス　　　　　　　　　　 --- 対応するホスト名

IPアドレス　　　　　　　　　　 --- 対応するホスト名

IPアドレス　　　　　　　　　　 --- 対応するホスト名

以下の監査項目に関して記載できない場合は理由をご記入ください。※本申請が承認されない場合があります

（記入例：パッケージ製品のため開発言語は公開されていない。）

※EOLのOS等を利用している場合、許可されません

サーバのOS(バージョンまで記載)

実行環境： Apache・Nginx・IIS・Tomcat・その他（ ）

開発言語： PHP・Java・Python・JavaScript・その他（ ）

サービス提供設備・ネットワーク接続の概略図

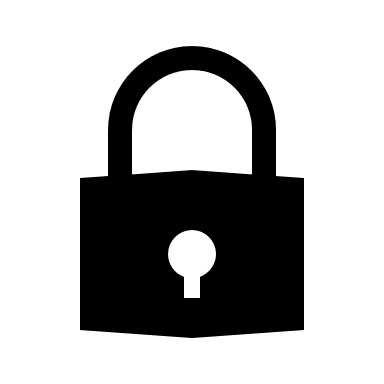
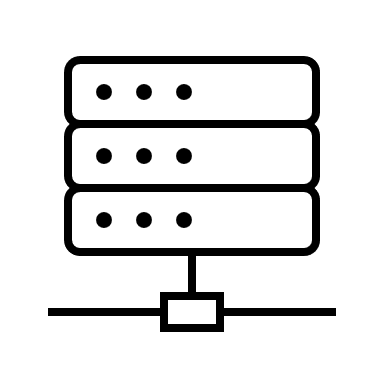
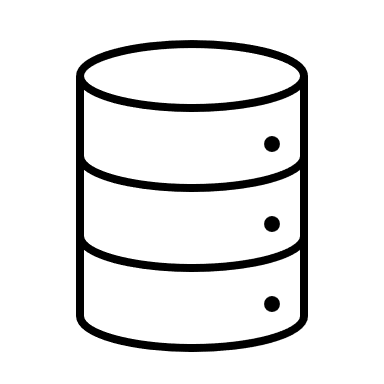
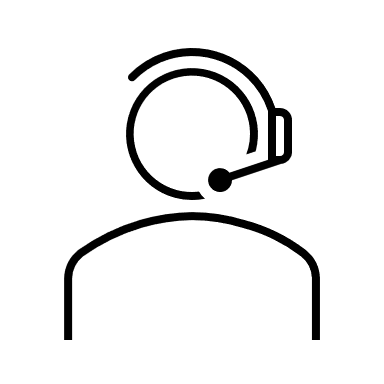
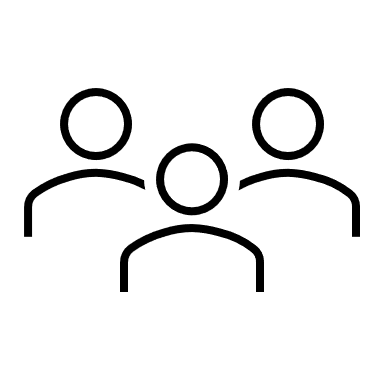
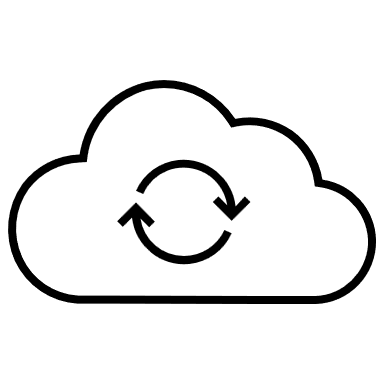
（設置場所，製品名，OS名など分かる範囲で併記してください）

サービス提供設備・ネットワーク接続の概略図（次の記載事項を含めてください）

* + - サービス内で使用しているサーバ、ファイアウォール、セキュリティ機器の構成
    - 利用者端末から当該サービスまでのネットワーク経路
    - 管理者端末から管理インタフェースまでのネットワーク経路
    - 機構LDAP、機構ADなどのサーバへの接続経路
    - 利用しているサービスの名称（例：名大仮想専用ホスティングサーバサービス）
    - 個人情報および機密性3以上（東海国立大学機構 情報格付け基準に基づく）の情報の保管場所

（設置場所，製品名，OS名など分かる範囲で併記してください）

例



個人情報

DBサーバ（物理サーバ）

SPサーバ（仮想専用ホスティングサービス）

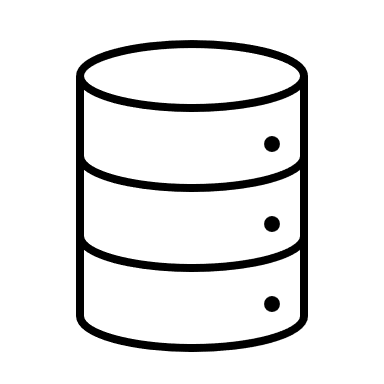
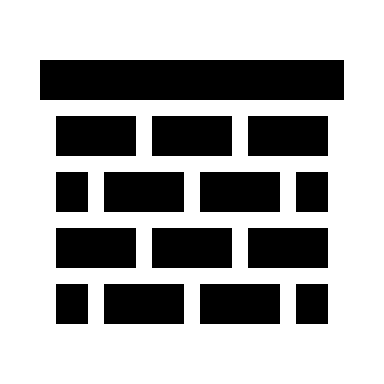
管理者

利用者

インターネット

NICE

専用FW



機構LDAP

**機構統合認証サービス利用チェックリスト**

項目ごとに該当する□を☑に置き換えてください

・東海国立大学機構統合認証サービス利用内規について

□責任者は東海国立大学機構統合認証サービス利用内規，および「本申請内容」を熟知している

□その他( )

・サービス公開範囲について（IPに基づきポートへのアクセス制限をしているかどうかを指します）

□サービスは機構内限定

□サービスは岐大限定

□サービスは名大限定

□サービスは制限なく公開している

□その他( ) ※本来は機構内限定にすべきだが何らかの理由で外部に公開している場合など

・サービスの脆弱性診断の実施状況について

※名大[ガイドライン「3.5 サーバ」「3.5.2 管理者の義務」「9.脆弱性検査」](https://icts.nagoya-u.ac.jp/ja/security/guideline.html)に関するものです。  
サービスの所属が岐大の場合、この回答は審査に影響しません。

（ 名大所属サービスで内容が不明の場合[情報セキュリティ室](https://icts.nagoya-u.ac.jp/ja/security_office/access.html)にお問い合わせください ）

□実施済みである(実施日 西暦\_\_\_年\_\_月\_\_日)

□実施予定である(実施日 西暦\_\_\_年\_\_月\_\_日)

□その他( )

・サービス管理について

□サービスは自身/自部局で完全に管理可能な状態にある

□サービスは機構外の関係者によって管理されている

□その他( )

・サーバ管理について

□サーバは自身/自部局で完全に管理可能な状態にある

□サーバは機構外の関係者によって管理されている

□その他( )

・サーバ物理所在地について

□サーバは機構内に設置されている

□サーバは国内に設置されている

□サーバは国外(国名:\_ \_\_)に設置されている

・システムの保守について

□サーバOSはEOLのものを利用していない  
※EOL(End of Life の略で重要なセキュリティアップデートなども含めあらゆるサポートが提供されないシステムやソフトウェアを指します)のOSを利用していたり、重大な脆弱性のあるシステムの機構統合認証の利用は認められません。  
 EOLの近いOSを利用しているサービスに置かれましては、移行計画についてご確認ください。

・個人情報データ管理について

□データはすべて東海国立大学機構個人情報保護規程に基づき厳密に管理されている

□その他( )

・個人情報データ利用範囲について

□データはすべて完全に機構内および機構内関係者のみによって扱われる

□データは機構外の関係者にも扱われる(第三者提供にあたらないもの)

□東海国立大学機構個人情報保護規程に基づく第三者提供を行う

□その他( )

---この項目は機構外関係者が存在する場合に回答してください-----------------------------------------------------

・機構外の関係者名（複数記載可）

　　　　　　　　　　　　　(例:○○株式会社)

・契約について

□機構外関係者とは必要な契約を正しく結んでいる。  
□その他( )

※必要な契約とは保守運用契約・業務委託契約・守秘義務契約・その他の機構外関係者が情報を取り扱う際に法律や規約上必要になるもの、また情報が適切に管理されることを保証するものを指します。

・関係者の管理について  
　□コントロール(ベンダーコントロール)が可能な状態にある

□その他( )

------------------------------------------------------------------------------------------------------------------------------------

・個人情報の利用について

□機構統合認証から得て保存した個人情報を、本人以外の人が参照可能な形で扱う

※後にある取得する属性の項目で「取得後の保存」を有りとしているほぼすべてのシステムが該当するものです。システムの仕様やログ等の確認など、本人以外が確認できる場合は例外なくチェックしてください。

------「個人情報の利用について」の項目にチェックした場合以下に回答してください---------------------

・保存した個人情報を参照する人(複数記載可)

所属および役職名 　　 名前 参照の目的

(所属および役職名 　　 名前 参照の目的 )二人以上いる場合行を追加してください

特定の個人以外が参照可能な場合その詳細

※どのような人が、どのような権限で、どのような情報を、どのように閲覧可能か説明すること

・該当の個人情報を扱う権限について

(例:東海国立大学機構個人情報保護規程「第2章 個人情報の保護体制」に基づく保護管理者や保護担当者の○○から信任を得た、など)(メモ:機構の個人情報利用に関するセキュリティクリアランス規定として)

記載欄

・個人情報を閲覧可能な人を、上に記載の人に限定する対策について

(対策の例:データを扱うパソコンにはパスワードを設定している。

パスワードをデスクに張り付けて置いたり、画面を開いたまま席を離れたりしていない。

データの共有は各関係者に個人情報管理におけるセキュリティを周知の上、ファイルのパスワード設定やNSSSなどを用いたセキュアな共有を行う。など)

□対策を行う

□対策を行わない

------------------------------------------------------------------------------------------------------------------------------------

以下は一部関連規定に関する項目です。遵守していない事例が見られたため、運用の適正化のため追加されました。もちろん以下のチェックリスト以外にも関連規定のすべての項目を厳密に順守している必要があります。各システム管理・担当者の皆様におかれましては、十分にご留意ください。

・個人情報ファイル簿への記載について

※データの取得元によらず、1000件以上の個人情報を保存しているすべてのシステムは個人情報ファイル簿に記載が必要です(東海国立大学機構個人情報保護規定 第31条)

□個人情報を保存していない

□999人以下の個人情報を保存している

□1000人以上の個人情報を保存しており、個人情報ファイル簿にシステムを記載している  
（記載名称 ）

※以下は個人情報の取得を行っていない場合、回答不要です

個人情報利用目的の制限(東海国立大学機構個人情報保護規定第12条)について

・利用目的は文書等で明確に定義されているか

□利用目的は文書等で明確に定義されている

□それ以外(詳細 )

・利用目的の範囲を超えた個人情報の取り扱いがないか

□利用目的の範囲を超えた個人情報の取り扱いがない

□それ以外(詳細 )

・利用の目的について本人に同意を得ているか（機構IDP属性確認画面は利用目的に対しての同意ではありません）

□利用目的を本人に伝え、同意を得ている

□それ以外(詳細 )

※以下は個人情報の取得を行っていない場合、回答不要です

個人情報利用目的の公表・通知(東海国立大学機構個人情報保護規定第15条)について  
・個人情報取得時に利用目的を本人に通知または公表しているか

□個人情報取得時に利用目的を本人に通知または公表している

□それ以外(詳細 )

**機構統合認証サービス-IdP**

1. 機構IdPの利用  
   利用する ／　利用しない

IdPの利用を行う場合，SPのメタデータの登録が必要です。  
メールで，SP**メタデータファイルをIdP管理者にお送りください**。  
SPメタデータファイルのご提出は、この申請書と同時である必要はありませんが、  
希望の登録日がある場合、遅くともその5営業日以前にご提出ください。

1. 機構IdPから取得する属性  
   注意:情報を取得する場合、個人情報に関する規定を理解し順守する必要があります。

https://education.joureikun.jp/thers\_ac/aggregate/catalog/index.htm

属性の保存を行う場合、理由と利用目的:

|  |  |  |
| --- | --- | --- |
| 属性名 (マニュアルをご参照の上、属性の正式な英語名をご記載ください) | 取得後の 保存 （有/無） | 備考 |
| 記載例: uid | 有 | ユーザー情報を管理するIDとして利用する |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

機構IdPで利用できる属性は下記URLの「機構統合認証サービス利用マニュアル」を参照してください。

https://icts.nagoya-u.ac.jp/ja/services/thers/thers-auth/thers-auth-service.html

1. 認証対象のフィルター  
   認証対象を身分により制限することが可能です。デフォルトは無制限です。  
   必要な場合、以下にご記載ください。  
     
   ・名古屋大学構成員のみ認証 ( )  
   ・岐阜大学構成員のみ認証 ( )

上記に無いフィルターをご希望の場合、ご相談ください

**機構統合認証サービス-LDAP**

1. 機構LDAPの利用  
   利用する ／　利用しない

LDAPを利用する場合、理由と利用目的:

1. 機構LDAPに接続するサーバの**グローバル**IPアドレス  
   　　　　　　　　　　　（複数記載可）
2. 機構LDAPから取得する属性

注意:情報を取得する場合、個人情報に関する規定を理解し順守する必要があります。

<https://education.joureikun.jp/thers_ac/aggregate/catalog/index.htm>

情報の保存を行う場合、理由と利用目的:

|  |  |  |
| --- | --- | --- |
| 属性名 ( LDAPスキーマ定義をご参照の上、属性の正式な英語名をご記載ください) | 取得後の 保存 （有/無） | 備考 |
|
| 記載例: uid | 有 | ユーザー情報を管理するIDとして利用する |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

機構LDAPで利用できる属性は下記URLの「【別紙】LDAPスキーマ定義\_機構統合LDAP」を参照してください。

<https://icts.nagoya-u.ac.jp/ja/services/thers/thers-auth/thers-auth-service.html>

注意:性別，生年月日，教職員戸籍氏名，学生氏名履歴は，基本的にSPへ提供されません。

必要な場合は、相応の理由を記載してください。

―――――――――――――――――――――――管理者記入欄―――――――――――――――――――――

BIND ID

受付日

作業日