情報基盤計算機システム　　一式

Computer Infrastructure System　　1 set

仕様書

2017年7月

京都工芸繊維大学

2017 年 7 月 19 日　16 時 26 分 版
main *Revision* : 1.5
abst *Revision* : 1.4
tetsuzuki *Revision* : 1.4
func-common *Revision* : 1.17
cis-services *Revision* : 1.8
cis-servers *Revision* : 1.2
cis-terminals *Revision* : 1.4
is *Revision* : 1.18
jim *Revision* : 1.7
lib *Revision* : 1.10
manage *Revision* : 1.4
resources *Revision* : 1.10

目 次

I. 仕様書概要説明

1　更新の背景及び目的

学内共同利用を目的とする情報科学センターで運用中のシステム, 情報の専門教育を目的とする情報工学課程・専攻で運用中のシステム, 学内事務業務の効率化の情報基盤としての本学事務局で運用中のシステム, および，図書館の電算処理の推進と学内外への情報提供を目的とする本学図書館で運用中のシステムのそれぞれを統合した情報基盤計算機システムは, 平成 26 年 3 月に導入されて以来ほぼ 3 年が経過した.

この間，教育・研究・事務・図書館の高度化及び多用化に伴う計算機需要は加速的に増大している．また，近年のインターネットの大衆化やモバイル環境の普及など，大学を取り巻くネットワーク環境も大きな変化を続けている．このため，情報セキュリティの強化・向上と利用環境の一層の整備を目的として，特に, 利用者原簿管理を含む認証基盤および運用管理基盤に重点を置きつつ, システム全体を更新する.

さらに, 学内で別途運用していた言語教育用パソコン教室 の更新時期にもあたるため, 運用管理の統一化をはかることを目的とし, 講義室汎用型演習システムとして併せて調達する.

2　調達内容

1. 導入計画物品及び数量
   情報基盤計算機システム一式 (搬入・据付・配線・調整・保守・撤去を含む．)

2. 調達方法
   賃貸借

3. 導入予定時期
   平成 29 年度第 4 ・四半期以降 (賃貸借期間: 48ヶ月)

4. 導入場所
   京都工芸繊維大学 松ヶ崎キャンパス内, 嵯峨キャンパス内 および 福知山キャンパス内

3　調達物品名及び構成内訳

情報基盤計算機システム 一式
(構成内訳)

(1) 共通サービス基盤システム ..... 1 式
(2) 共通サーバ基盤システム ..... 1 式
(3) 共通クライアントシステム ..... 1 式
(4) 貸出用機器群 ..... 1 式

(5) 管理業務システム群 ..... 1 式

(6) 情報工学サブシステム ..... 1 式

(7) 事務局サブシステム ..... 1 式

(8) 図書館サブシステム ..... 1 式

以上の搬入，据付，配管，配線，調整，保守，借上げ期間満了または解約に伴う機器の撤去を含む.

4 技術的要求要件の概要

1. 本調達物品に係る性能，機能及び技術等（以下「性能等」という.）の要求要件（以下「技術的要件」という.）は別紙「調達物品に備えるべき技術的要件」に示すとおりである.
2. 技術的要件は全て必須の要求要件である.
3. 必須の要求要件は本学が必要とする最低限の要求要件を示しており，入札機器の性能等がこれを満たしていないとの判定がなされた場合には不合格となり，落札決定の対象から除外する.
4. 入札機器の性能等が技術的要件を満たしているか否かの判定は，情報基盤計算機システム技術審査職員において，入札機器に係る技術仕様書を含む入札説明書で求める提出資料の内容を審査して行う.

5 提出書類

システムの構成理念・特徴を述べ，次の各項について具体的に記述した提案書を 11 部作成の上，提出すること．また, カタログ以外については，電子データ (PDF 形式) でも提出すること．なお, 電子データは, 1 式で良いが, オフラインで参照することができ, かつ, 複製禁止処理は施さないこと.

1. システム提案書
2. ハードウェア及びソフトウェアの機能・構成・性能及び規格
3. システム構成機器の寸法，重量，所要電力，発熱量，騒音
4. システム構成機器に必要な電源の仕様
5. システム構成機器のネットワーク相互接続の様態
6. 機器設置場所におけるシステム構成機器レイアウト案
7. システムの搬入・据付・調整・検査を含む，現行システムからの移行日程表
8. システムの保守内容とその体制，ならびに運用支援体制
9. ハードウェア及びソフトウェアのカタログ

10. システム構成機器等のレンタル料金 (定価) 表
11. 消耗品に関する資料
12. 納入実績表

6 その他

1. 技術仕様等に関する留意事項
    a. 提案する機器及びソフトウェアは，原則として入札時点で製品化されていること．入札時点で製品化されていない機器又はソフトウェアによって応札する場合には，技術的要件を満たすことを証明する資料及び納入期限までに製品化され納入することを保証する確約書を提出すること．なお，これらの成否は情報基盤計算機システム技術審査による．
    b. 要求要件で言語指定を明記していないとき，ソフトウェアが複数の言語に対応している場合は，日本語に対応するソフトウェアが存在しない場合を除いて，日本語版を提供すること．
2. 導入に関する留意事項
    a. 導入時の作業日程と体制を提示し，本学と協議し，その指示に従うこと．
    b. 導入システムは，平成30年3月1日より運用を開始する (レンタル期間: 48ヶ月).
3. 提案に関する留意事項
    a. 提案書は日本語で作成すること．
    b. 提案に際しては，提案システムが本仕様書の要求要件をどのように満たすか，或いは，どのように実現するかを要求要件ごとに具体的かつわかりやすく，資料等を添付する等して説明すること．
    c. 提案する機器のファームウェア及びソフトウェアの中で，納入期限までにバージョンアップが予想される場合，その予定時期等が記載された資料を提出すること．
    d. 提案された資料等が不明確であると，情報基盤計算機システム技術審査職員が判断した場合は，技術的要件を満たしていないとみなす．
    e. 提出された内容等についてヒアリングを行う場合があるので，誠実に対応すること．
    f. 提案資料等に関する照会先を明記すること．
4. その他の留意事項
    a. 本調達には，ハードウェアおよびソフトウェアの保守費用を含む．
    b. 搬入，据付，配線，調整，既存設備との接続 (既存設備の設定変更を含む) ならびに既存設備からのデータ移行に要する全ての費用は，本調達に含む．

c. 解約及び借入期間満了時には借入物品を撤去すること．なお，撤去に要する全ての費用は本調達に含む.

II. 調達物品に備えるべき技術的要件

(性能，機能に関する要件)

1　共通サービス基盤システム群

注: 特別指定が無い限り，各サービスを構成する全てのサーバ・ストレージ領域・ネットワークは，共通サーバ基盤システム群上で動作すること．

また, 設定は, Ansible 相当以上の構成管理システムで集中管理すること．

★ Ansible Tower 相当以上と判断される管理機能を有する場合は, 加点として評価する．

1.1　利用者原簿管理システム 1 式

1-1-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．

1-1-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること．

1-1-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること．

1-1-4. アクセスログをサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1-1-5. 外部データソース連携ログをサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1-1-6. 独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしてもサービスが停止しない構成であること．

1-1-7. マスターデータベースのデータは，すべて暗号化されたファイルシステム上に保管して動作する機能を有すること．ただし，暗号化の為に使用する秘密鍵は，盗難に配慮した取り外し可能なメディア上に保管されており，かつ，サービスの再始動にあたって人手を介することなく稼働する機能を有すること．

1-1-8. 原簿情報の変更について監査ログを保存する機能を有すること．
★ 原簿情報の閲覧について監査ログを保存する機能を有する場合は加点として評価する

1-1-9. Web GUI の通信は全て https で行うこと．

1-1-10. 現行の利用者管理システム (SyntheUMS) 上にある全ての利用者情報を移行すること．なお，現行の利用者管理システムからの利用者情報の出力は本学にて行うものとする．

1-1-11. 調達に含まれる全端末パソコンからの同時のパスワード変更操作に対して最大 1 分以内での応答性能を有し，操作時に稼働している連携先の外部データソースへの配信を最大 5 分以内で行う性能を有すること

1-1-12. 利用者情報を管理するマスターデータベース機能を有すること．ただし，利用者情報の属性は，表 1 のものを含み少なくとも 120 項目を区別して保持する機能を有すること．

1-1-13. ODBC/JDBC 相当の API でマスターデータベースにアクセスできること．

1-1-14. Unicode で記述されたユーザ属性を取り扱えること．

1-1-15. 「氏名 (母国語表記)」の項目は Unicode で 64 文字以上保持できること (注：Unicode において 1 文字は 1 バイトとは限らない)

1-1-16. パスワードハッシュ方式が識別できる形式で各ユーザのパスワードハッシュを保持する機能を有すること．

1-1-17. システム管理者の操作でユーザ属性項目の追加が可能であること．

1-1-18. マスターデータベースは 12,000 名以上の利用者情報を管理可能であること．

1-1-19. 各サービス上のユーザ識別に用いる ID(以下, userID) と，サービスの利用主体である個人を識別するための ID(以下, personID) を区別して保持する機能を有すること．

1-1-20. personID のみを有し，userID を持たない利用者の情報も取り扱える機能を有すること．

1-1-21. userID のみを有し，personID を持たない利用者の情報も取り扱える機能を有すること．

1-1-22. GUI と CLI によるユーザ登録/変更/削除の機能を有すること．
★ 本学内の複数の部署から，それぞれが掌握するユーザ群に対して，追加，更新，一時停止，削除，有効期限設定ができる機能を有する場合は加点として評価する．

1-1-23. 指定した検索キーに該当するユーザアカウントの一覧を表示する管理者向け画面を有すること．なお，検索キーとして少なくともログイン ID，姓，名を指定できること

1-1-24. マスターデータベースから利用者情報を削除することなく，利用者に対応するアカウントを無効化する機能を有すること．また，一度無効化したアカウントを再有効化する機能を有すること．

1-1-25. 本システムで入出力する CSV ファイル (Character-Seperated-Value) の形式は，少なくとも RFC4180 に準ずる comma-seperated-value と MIME Type tab-separated-values (https://www.iana.org/assignments/media-types/text/tab-separated-values) で規定される tab-seperated-value に対応するものとする．
★ システム管理者によってフィールドの区切り文字を任意に変更できる機能を有する場合は，加点として評価する

1-1-26. 外部データソース (CSV ファイル,LDAP,ActiveDirectory,ODBC/JDBC 相当の API を持つリレーショナルデータベース) からデータを取り込み, マスターデータベース上の利用者情報に反映する機能を有すること (または同等機能の実装が可能な開発キットを有すること).
★ REST API を持つ外部データソースと連携する機能を有する場合は加点として評価する

1-1-27. また, システム管理者の操作によって, データ取り込み時に項目の対応付け, 文字列の連結, 正規表現によるパターンマッチを用いた部分文字列の切出し・置換操作が行えること (または同等機能の実装が可能な開発キットを有すること).

1-1-28. 各ユーザ属性項目毎に利用禁止文字あるいは利用可能文字を正規表現を用いて指定する機能を有し, 条件に合致しないデータを受付けない機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-29. また, 条件に合致しなかったデータの内容及び処理時刻を管理者ログとして記録する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-30. 連携先の LDAP サーバ,ActiveDirectory サーバに対する更新要求の前後に，連携先のサーバ上であらかじめ指定されたコマンドを実行し，その結果を収集する機能を有すること.

1-1-31. アカウントの無効化・再有効化情報を外部データソースに 10 分以内に反映させる機能を有すること.

1-1-32. CLI によって，利用者の属性の変更を実施する機能を有すること.
★ マスターデータベースと連携先の全ての外部データソースに変更が反映されたかどうか の状況を応答する機能を有する場合は加点として評価する

1-1-33. 外部データソースとの通信方式は公開鍵認証を用いた暗号化通信に相当すると判断される方式であること

1-1-34. 外部データソースからのデータ取り込み時に, 半角カナを含むデータを取り込む機能を有すること.

1-1-35. 外部データソースからのデータ取り込み時に, 和暦表記 (例：平成２９年６月１日) の日付を西暦表記の日付に変換して取り込む機能を有すること.

1-1-36. 下記の機能を有する，ユーザグループ管理機能を有すること.

1-1-36-1. 外部データソース (CSV ファイル,ODBC/JDBC 相当の API を持つリレーショナルデータベース) からグループのマスター情報を取り込む機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-36-2. 外部データソース (CSV ファイル,LDAP,ActiveDirectory,ODBC/JDBC 相当の API を持つリレーショナルデータベース) からデータを取り込み, ユーザ属性に基づいてグループのメンバーに反映する機能を有すること (または同等機

能の実装が可能な開発キットを有すること).
★ REST API を持つ外部データソースと連携する機能を有する場合は加点として評価する

1-1-36-3. グループ属性項目毎に利用禁止文字あるいは利用可能文字を正規表現を用いて指定する機能を有し, 条件に合致しないデータを受付けない機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-36-4. また, 条件に合致しなかったデータの内容及び処理時刻を管理者ログとして記録する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-36-5. 既存のメーリングリストのメンバー情報をユーザ属性・グループ情報として取り込むこと.

1-1-36-6. 各ユーザグループに対し, 所属するユーザのメールアドレス一覧を CSV 形式で出力する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-36-7. 各ユーザグループに対してメンバーの追加・更新・削除権限を持ったグループ管理者を割当てる機能を有し，グループ管理者によるメンバー管理作業が行えること

1-1-36-8. 本システムで定義されたグループに対し, 和・積・差の集合演算を施した合成グループを定義する機能を有すること.

1-1-36-9. ユーザが所属するグループとグループに所属するユーザの整合性を自動的に保つ機能を有すること.
★ 各サービス上のユーザ識別に用いる ID(userID) に基づいて定義されたグループを, 個人識別用の ID(personID) で定義されたグループに変換する機能を有する場合は加点として評価する.

1-1-36-10. グループ一覧を出力または表示する管理者向け機能を有すること. なお, グループ属性および所属ユーザを検索キーとして指定できること.

1-1-37. REST API を通じて以下の操作が可能な機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-37-1. ユーザの追加/削除/有効化/無効化

1-1-37-2. ユーザ属性の追加/更新/削除/取得

1-1-37-3. グループの追加/削除

1-1-37-4. グループ属性の追加/更新/削除/取得

1-1-37-5. グループメンバーの追加/削除/取得

1-1-38. ユーザ属性・グループ属性に対する条件に基づき, 該当するユーザ・グループの情報のみを外部データソース (CSV ファイル,LDAP,ActiveDirectory,ODBC/JDBC 相当 の API を持つリレーショナルデータベース) に出力する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-39. ユーザ属性・グループ属性に対する条件に基づき, 該当するユーザ・グループの情報のみを外部データソース (CSV ファイル,LDAP,ActiveDirectory,ODBC/JDBC 相当 の API を持つリレーショナルデータベース) から削除する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-40. 外部データソースとの連携において, ユーザ属性・グループ属性に対する条件を属性項目の組み合わせや正規表現一致によって指定する機能を有すること (または同等機能の実装が可能な開発キットを有すること).

1-1-41. 外部データソースとの連携において, システム管理者の操作によって, データ出力時の項目の対応付けや文字列の連結, 正規表現によるパターンマッチを用いた部分文字 列の切出し・置換操作が行えること (または同等機能の実装が可能な開発キットを有すること).

1-1-42. システム管理者の操作により, 外部データソースの追加・削除が可能であること.

1-1-43. システム管理者が前もって設定した同期タイミング, ユーザ属性・グループ属性に対する条件, データの同期先情報に基づき, 該当するユーザ・グループの情報を外部データソース (LDAP, ActiveDirectory, ODBC/JDBC 相当の API を持つリレーショナルデータベース) に自動で同期する機能を有すること.

1-1-44. システム管理者が前もって設定したユーザ属性・グループ属性に対する条件, データの同期先情報に基づき, 該当するユーザ・グループの情報を外部データソース (LDAP, ActiveDirectory, ODBC/JDBC 相当の API を持つリレーショナルデータベース) に一括同期する機能を有すること.

1-1-45. システム管理者が前もって設定したユーザ属性・グループ属性に対する条件, データの同期先情報に基づき, 該当するユーザ・グループの情報を外部データソース (LDAP, ActiveDirectory, ODBC/JDBC 相当の API を持つリレーショナルデータベース) に適用させる操作を即座に実行開始させる API を有すること.

1-1-46. 連携先の外部データソースのうち，一部または全部が停止もしくは異常状態に陥っていたとしても，復帰後に，停止中/異常状態中の全ての操作を再実行させることができること.
★ 復帰後 10 分以内に，停止中/異常状態中の全ての操作が，順序に従って実行される機能を有する場合は加点として評価する

1-1-47. 統合認証システムが利用者原簿管理システム上のユーザ・グループ情報に同期した認証・認可機能を提供できるように, 外部データソースとの連携が設定されていること

1-1-48. 文字表現の異なる外部データソースとの通信にあたって，少なくとも，UTF-8，Shift-JIS，EUC-JP の文字コード間の相互変換機能を有すること.

1-1-49. 本学の人事労務課の職籍データベース (U-PDS) から，あらかじめ指定された項目を取り出したファイルを自動的に取得し，マスターデータベースに反映する機能を

有すること．なお，職籍データベースとの間の通信は，専用の VLAN もしくは SSL 通信相当以上と判断される方式であること．

1-1-50. 本学の学務課の学籍データベース (DreamCampus) から，あらかじめ指定された項目を取り出したファイルを自動的に取得し，マスターデータベースに反映する機能を有すること．なお，学籍データベースとの間の通信は，専用の VLAN もしくは SSL 通信相当以上と判断される方式であること．

1-1-51. Web GUI と CLI によって，利用者のパスワード変更を実施する機能を有すること．
★ マスターデータベースと連携先の全ての外部データソースに変更が反映されたかどうかの状況を利用者に対して応答する機能を有する場合は加点として評価する

1-1-52. ユーザの一括登録時に，利用者毎に相異なるランダムな文字列と当該利用者の PIN 番号属性からなるパスワードを自動的に生成し，アカウント名とランダムな文字列部分をペアにして出力する機能を有すること．

1-1-53. 管理者が，強制的にパスワードを更新する機能を有すること．そのとき，パスワードとしてランダムな文字列を自動生成する機能を有すること．

1-1-54. また管理者が強制的にパスワードを更新した際, パスワード強制変更ログ (変更日時, 管理者作業を行ったユーザ・端末, パスワード変更対象となったアカウントの情報を少なくとも含む) を記録する機能を有すること

1-1-55. パスワード強制変更ログの閲覧・検索を管理者が行える機能を有すること
★ Web ブラウザ上で同等の作業を行える場合は加点として評価する

1-1-56. パスワード変更の際に，パスワードポリシー (特定文字 (列) の使用禁止，最小最大長，混在するべき文字種類の規定) をあらかじめ設定し，自動的にチェックして，使用できないものであればその旨を応答する機能を有すること．

1-1-57. 各ユーザが Web ブラウザ上で自身のパスワードを変更できる機能を有し, パスワード変更時にパスワードポリシーを強制する機能を有すること．

1-1-58. CLI によって，ランダムに生成した文字列を指定したトークンとして振り出して利用者属性を更新し，連携する外部データソースに渡す機能を有すること．

1-1-59. システム管理者の操作で各ユーザの公開鍵ならびに電子証明書を登録可能であること．
★ 各ユーザが自身で公開鍵を登録できる機能を有する場合は加点として評価する．

1-1-60. 各ユーザが自身のユーザ属性・所属グループを参照する機能を有し, かつ, 一般ユーザに公開するユーザ属性・所属グループの範囲をシステム管理者によって制限する機能を有すること．

1-1-61. e-Learning システム上のオンライン試験合否状況をユーザ属性情報または所属グループ情報にサービス利用資格として取り込む機能を有すること．

1-1-62. また, 合否状況の取り込み対象となるオンライン試験は追加・変更が可能であること

1-1-63. 利用資格を持つサービスに対して各ユーザが Web ブラウザ上でアカウント登録操作を行なえること.

1-1-64. 各ユーザが Web ブラウザ上で自分が利用資格を持つサービスの一覧を確認できる機能を有すること.

1-1-65. ユーザのアカウント登録操作に対して該当システム上にアカウントを随時自動登録する機能を有すること.

1-1-66. 一般ユーザの操作画面については，日英切替え表示または日英併記が可能であること.

表 1: マスターデータベース項目

項目名	説明
アカウント名(userID)	システム上の識別子(16 文字以上に対応すること)
統一アカウント名(personID)	アカウント名(userID)に対応する個人識別用ID(英数字16文字以上)
外部クラウドサービス用ID	Office365用ImmutableID(Active DirectoryのobjectGUID値)
本パスワード	本人用のパスワードハッシュ
トークン	システムが自動付与するパスワード(少なくとも7種類以上)
HOTP/TOTPトークンシリアル番号	英数字12文字以上
電子メール	アドレスドメインを含む(foo@kit.ac.jp, bar@edu.kit.ac.jp)
転送先電子メールアドレス	アドレスドメインを含む(foo@docomo.ne.jp)複数のメールアドレス
個人番号	学籍番号(学生)，職員番号(教職員)
氏名(母国語表記)言語ロケール	母国語表記の言語ロケール
氏名(母国語表記)	姓とそれ以外の間に半角スペースを入れて管理する(Unicode64文字以上)
氏名(ローマ字表記)	姓とそれ以外の間に半角スペースを入れて管理する
通称(日本語表記)	姓とそれ以外の間に半角スペースを入れて管理する
PIN	情報初期パスワード生成時に利用する
uidNumber	UNIX システム利用時のUID(64bit以上)
gidNumber	UNIX システム利用時のGID(64bit以上)
LoginShell	UNIX システム利用時のログインシェル
homeServer	UNIX システム利用時のファイルサーバ名
homeDirectory	UNIX システム利用時のホームディレクトリのパス
SSH 公開鍵	SSHv2 用公開鍵
電子証明書	X.509証明書(Base64エンコーディング)
NFCカードID	オンデマンド印刷複合機用カードID
大学/大学院	
学部	
研究科	
部局	
学域	
学系	
課程	
専攻	
学年	
部門	
職種	
指導教員	
在籍ステータス	例: 在学・休学・卒業・除籍(学生)
事務所属課	
事務所属係	
登録年月日	システムに登録された年月日(unix 64bit timestamp相当)
削除年月日	システムで自動的に削除する年月日(unix 64bit timestamp相当)
最終更新タイムスタンプ	システム上の属性が最後に変更された日時(unix 64bit timestamp相当)
有効化状態	アカウントの有効/無効状態フラグ
有効化年月日	システムで自動的に有効化する年月日(unix 64bit timestamp相当)
無効化年月日	システムで自動的に無効化する年月日(unix 64bit timestamp相当)
備考欄	自由記述欄

1.2 統合認証システム 1 式

1-2-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．なお, プロプライエタリな認証サーバの為に専用サーバを一部に用いて実現しても良い.

1-2-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること．ただし，Windows 系の OS での提案の場合は，通信路が 128bit 以上の暗号化鍵で暗号化されたリモートデスクトップサービスで代替しても良い.

1-2-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること.

1-2-4. アクセスログをサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること.

1-2-5. 認証履歴をサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること.

1-2-6. 独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしても各認証サービスが停止しない構成であること.

1-2-7. 各認証サービスを停止することなく保守が可能な構成であること.

1-2-8. 少なくとも，以下のプロトコルに対応する認証・認可サービスを提供する機能を有すること.
SAML 2.0/CAS 3.0/Active Directory/LDAP v3/RADIUS
★ SAML 認証および CAS 認証に非対応の Web サービスに対して，リバースプロキシ型の代理認証機能を有する場合は，加点として評価する.
★ リスクベース認証機能を有する場合は, 加点として評価する.

1-2-9. ユーザ属性によって認可するユーザ群を限定する機能を有すること.

1-2-10. 国立情報学研究所学術認証運営委員会の定める「学認技術運用基準 (ver. 2.1)」を満たす SAML IdP の運用が可能であること.

1-2-11. 利用者原簿管理システムから出力されたユーザ・グループ情報を取り込む機能を有すること

1-2-12. Unicode で記述されたユーザー属性を取り扱えること.

1-2-13. 利用者原簿管理システム上のユーザ・グループ情報に同期した認証・認可機能を提供するように設定されていること.

1-2-14. 利用者原簿管理システム上で無効化状態にあるアカウントに対する認証を拒否するように設定されていること

1-2-15. 各サービス上のユーザ識別に用いる ID(以下, userID) による認証に加え, サービスの利用主体である個人を識別するための ID(以下, personID) による認証が可能であること.

1-2-16. userID, personID 合わせて 12,000 アカウント以上に対する認証・認可サービスを提供できること

1-2-17. userID で認証を行い, 対応する personID のアカウント情報を認証結果として送出する機能を有すること.
★ personID を用いた SAML 認証または CAS 認証において, personID に紐付けられた userID アカウントの候補から利用者が対話的にアカウントを選択し, 選択したアカウントを認証結果として返す機能を有する場合は加点として評価する.

1-2-18. SAML 認証において Shibboleth IdP 3.2 相当以上のユーザ属性出力機能を有すること.

1-2-19. SAML 認証において, オプトイン方式によるサービス利用規約の同意取得ならびにユーザ属性送信の同意取得を実施する機能を有すること. また, ユーザからの同意取得結果をリレーショナルデータベースに保存するように設定されていること.

1-2-20. SAML 認証においては少なくともパスワード認証に対応すること.
★ HOTP または TOTP 方式のワンタイムパスワードを用いた二要素認証に対応する場合は加点として評価する.

1-2-21. 表 2 に示す認証サービスの提供に必要な LDAP サーバ,Radius サーバ,ActiveDirectory サーバが稼動すること

1-2-22. OpenLDAP 2.4 または 389Directory Server 1.3.6 相当以上と判断される LDAP サーバプログラムを有すること.

1-2-23. LDAP サーバはユーザが所属するグループとグループに所属するユーザの整合性を自動的に保つ機能を有すること.

1-2-24. FreeRadius 3.0 相当以上と判断されるサーバプログラムを有すること.

1-2-25. Microsoft Active Directory と判断されるサーバプログラムを有すること.

なお, Active Directory サーバは Microsoft 社 Windows Server 2012 相当以上のオペレーティングシステム上で稼働するシステムであること.

1-2-26. 予め指定された頻度以上の認証失敗を検出する機能を有すること.

1-2-27. 利用者の Web ブラウザに対して, 認証情報を機器に覚えこませて自動入力させることを避ける仕組みを有すること.

1-2-28. Web クライアント用の認証情報入力画面において, クライアントとの通信には HTTPS を用いること.

1-2-29. 一般ユーザの操作画面については, 日英切替え表示または日英併記が可能であること.

1-2-30. LDAP クライアントとの通信は SSL で暗号化されていること.

1-2-31. 本認証システムを用いた認証の利用状況について認証ログを集中管理できる機能を有すること.

1-2-32. 各ユーザが自身のアカウントの最新の SAML 認証履歴 (認証日時と認証の成否) を参照する機能を有すること.

★ LDAP,ActiveDirectory の認証履歴についても参照する機能を有する場合は加点として評価する.

★ 過去 30 回以上の認証履歴について参照する機能を有する場合は加点として評価する.

表 2: 認証サービス一覧

認証サービス名	マスタ DB 項目	用途・認証対象
LDAP1	本パスワード	全構成員用
	SSH 公開鍵	全構成員用
LDAP2	本パスワード	情報工学教育関係者用
LDAP3	本パスワード	事務局関係者用
LDAP4	本パスワード	図書館関係者用
LDAP5	トークン 1	ファイル共有システム用
LDAP6	トークン 2	電子メールシステム用
LDAP7	トークン 3	認証付きコンテンツ管理システム用
RADIUS1	本パスワード	全構成員用
RADIUS2	本パスワード	情報工学教育関係者用
RADIUS3	本パスワード	事務局関係者用
RADIUS4	本パスワード	図書館関係者用
RADIUS5	トークン 4	ネットワーク接続認証システム用 (全構成員用)
RADIUS6	トークン 5	ネットワーク接続認証システム用 (情報工学部門関係者用)
RADIUS7	トークン 6	VPN ブラウザ接続確認用 (既設 Fortigate1000C)
RADIUS8	トークン 7	VPN トンネル接続確認用 (既設 Fortigate1000C)
ActiveDirectory1	本パスワード	全構成員用
ActiveDirectory2	本パスワード	情報工学教育関係者用
ActiveDirectory3	本パスワード	事務局関係者用
ActiveDirectory4	本パスワード	図書館関係者用

1.3 統合運用管理システム 2 式

注: 本サーバ監視システムは，2.3 節の仕様を満たした装置で, かつ, 本節記載の機能・性能要件をすべて満たすように構成した上で, 情報科学センター 112A 号室とショウジョウバエ遺伝資源センター 106 号室に 1 セットずつ配置すること.

1-3-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること.

1-3-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること.

1-3-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること.

1-3-4. zabbix 3.0 相当以上と判断されるサーバ監視プログラムを有すること.

1-3-5. syslog-ng もしくは rsyslog 相当以上と判断されるログサービスプログラムを有すること.

1-3-6. 本システムの全てのサーバのログ情報に対して, 区別して収集し, 一定期間ごとに圧縮し, 不要になったものを削除し, elastic search や kibana 相当以上と判断されるアプリを利用してログを分析する機能を有すること.

1-3-7. 本システムの全てのサーバの設定情報に対して, Ansible などと連携し, 設定情報をリポジトリ化してバージョン管理したり, 複数世代のバックアップを保存する機能を有すること.

1-3-8. 蓄積したログは，2.5 項のバックアップストレージに自動的に移動する機能を有すること．ただし，移動したログファイルは，本監視システムから NFS などのファイル共有サービスを用いて参照する機能を有すること.

1-3-9. サーバ毎に指定のユーザおよびグループに属している利用者に監視を移譲できる機能を有すること.

1-3-10. 本提案の構築に含む, 既設 KITnet4 ならびに KITnet5 の機器を監視対象に含める機能を有すること．なお，KITnet4 は NEC 製 NetVisor，KITnet5 は zabbix 2.2 による監視機能が存在しているので利用して構築しても良い.

1-3-11. 情報科学センター 112A 号室もしくは ショウジョウバエ遺伝資源センター 106 号室のいずれかのサーバ監視システムが停止したとしても，他方のサーバ監視システムが監視を継続する機能を有すること.

1-3-12. 既設 KITnet4 もしくは KITnet5 のいずれかが停止したとしても，停止していない側のネットワークとそれに直接接続している機器に対して，監視を継続する機能を有すること.

1-3-13. 予め指定されたパターンのログを自動的に検索し，それを外部に報告する機能を有すること．

1-3-14. 予め指定された間隔で，収集されたログを自動的に圧縮保存する機能を有すること．

1-3-15. メディアあたり 4GBytes 以上の容量を有する WORM メディア書込み機能を有し，予め指定された間隔で，収集されたログを自動的に WORM メディアにコピーする機能を有すること．
※ WORM メディアの交換は, 手動で構わない.

1.4 e-Learning システム 1 式

1-4-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．

1-4-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること．

1-4-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること．

1-4-4. アクセスログを サーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1-4-5. Web サービス部とデータベース部は，それぞれ独立した 2 つ以上のサーバインスタンスで構成されており，負荷分散と冗長化の機能を兼ね備え，1 つのインスタンスが停止したとしてもサービスが停止しない構成であること．

1-4-6. 参照系サービスを停止せずにコンテンツのバックアップが可能であること．

1-4-7. 実運用に供するシステムとは独立して，モジュール開発ができる構成であり，かつ，開発成果は実運用に供するシステムへの連携が可能な構成であること．

1-4-8. 現在運用中の Moodle システム (Moodle 2.7) 上に存在する全てのコース (メタコース, コースを跨ぐリンクを含む) を移行すること．

1-4-9. 調達に含まれる全端末パソコンから学生ロールでの同時 300 アクセスに対して，以下の応答性能を有すること．

1-4-9-1. ユーザ名とパスワードを入力から遷移すべき画面が表示されるまで，最大 3 秒以内であること．

1-4-9-2. コース内のリソースのリンクをクリックしてから表示されるまで，最大 1 秒以内であること．

1-4-9-3. 課題の提出，小テストの完了ボタンをクリックしてから処理完了のページが表示されるまで，最大 3 秒以内であること．ただし，ファイルのアップロードを伴う操作については，利用者あたり最大 2Mbyte までの場合とする．

1-4-10. Moodle 3.1 相当以上と判断される Web をベースとする e-Learning システムであること.
★ Web ブラウザ上で BigBlueButton1.0 相当以上のオンライン会議を実施する機能を有する場合は加点として評価する
★ SafeExamBrowser バージョン 2.1 相当以上の Web ブラウザと連携し, 利用可能な機能を制限したデスクトップ環境でオンライン試験を実施する機能を有する場合は加点として評価する

1-4-11. 少なくとも日本語および英語の Web クライアント用操作画面を有すること

1-4-12. また, ユーザ操作により操作画面の表示言語を切替えられること

1-4-13. 少なくとも 50,000 コースを扱う機能を有すること.

1-4-14. コースの作成・削除，コース利用者の登録・削除などの管理作業について，バッチ処理が可能であること.

1-4-15. コースの自動バックアップ機能を有すること.

1-4-16. 内部データの参照関係を保ったまま，システム上に存在するアカウントのログイン ID 属性を一括して変更する機能を有すること

1-4-17. IMS Global LTI 1.1 規格に基づいて外部システムと連携する機能を有すること

1-4-18. 指定コースにおける履修者のオンライン試験合否状況を REST API またはデータベース連携を通じて外部システムに通知する機能を有すること.

1-4-19. 統合認証システムと連携した SAML 認証によるシングルサインオンが可能であること.

1-4-20. 認証情報入力画面における通信には HTTPS を用いること

1-4-21. 認証時に統合認証システムから受信するユーザ属性情報を (e-Learning システムにおける) ユーザ属性・所属グループ・システム利用資格に反映させる機能を有すること

1-4-22. 利用者原簿管理システム上のユーザ属性と同期を行う機能を有すること

1-4-23. 利用者原簿管理システムに登録されている全てのユーザが使用可能であること．ただし，利用者原簿管理システムからユーザが削除された場合でも，コース管理者が該当ユーザの過去のコース利用状況を参照することができる機能を有すること.

1-4-24. 利用者原簿管理システムにおいて personID のみを有し, userID を持たないユーザも利用可能であること

1-4-25. 電子メールシステムと連携し，e-Learning システム内のメッセージ交換サブシステムと電子メールの配送・転送先設定を連携させる機能を有すること.

1-4-26. コースインポート時に選択する担当コースをコース名により絞り込む機能を有すること．
★ コースインポート時に選択する担当コースをコース名順に表示する機能を有する場合は加点として評価する．

1-4-27. データベース機能におけるエントリー承認/非承認切り替え機能を有すること．

1-4-28. フォーラム機能におけるディスカッションのタイトル一覧表示/ネスト表示切り替え機能を有すること．

1-4-29. 受講登録キー入力画面で表示される教員名を任意に指定可能にする機能を有すること．

1-4-30. 本学の学務課の教科データベースから，あらかじめ指定された項目を取り出したファイルを自動的に取得し，コースとコースの受講者の設定に随時反映させる機能を有すること．なお，教科データベースとの間の通信は，専用の VLAN もしくは SSL 通信相当以上と判断される方式であること．

1-4-31. 少なくとも，コース登録ユーザの一覧，課題提出一覧，小テスト受験結果，評定を教師ロールで表示する際に，ログイン名もしくは学籍番号を表示し，また，並べ替えて表示する機能を有すること．

1.5 統合電子メールシステム 1 式

1-5-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．

1-5-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること．

1-5-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること．

1-5-4. メール配送ログ，メール読み書きログ，エラーメールログをサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1-5-5. 独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしてもサービスが停止しない構成であること．

1-5-6. 少なくとも 35 種類のメールドメインを区別して運用管理する機能を有すること．

1-5-7. 1.2 節の認証システムと連携して，ユーザ認証する機能を有すること．

1-5-8. 8,000 以上のユーザアカウントを使用する機能を有すること．

1-5-9. https を使用してブラウザでアクセスする Web メールサービスを有し，1.2 節の認証システムとの間で，Shibboleth シングルサインオンの機能 (SP) を有すること．なお，必要となる SSL 証明書およびその取得手続きは本調達に含む．

1-5-10. 本システム側で実行するメールのフォルダ振り分け機能を有すること．

1-5-11. 本調達に含まれる全ての端末パソコンからのIMAPv4rev1 (RFC3501, imaps), POP3 (RFC1939, pop3s) による同時アクセス可能なメールボックスアクセス機能を有すること．なお，必要となるSSL証明書およびその取得手続きは本調達に含む．ただし，認証には，1.2節の認証システムで用意された電子メール専用のLDAPを用いること．

1-5-12. 本調達に含まれる全ての端末パソコンからのSMTP (RFC5381, smtps), SMTP AUTH (RFC4954, submission) による同時アクセス可能なメールの送受信機能を有すること．なお，必要となるSSL証明書およびその取得手続きは本調達に含む．ただし，認証には，1.2節の認証システムで用意された電子メールシステム用のLDAPを用いること．

1-5-13. 1.2節の認証システムでアカウントの停止処理をした場合, 当該ユーザに対するメールサーバの送信時認証が通らないように連携する機能を有すること．

1-5-14. GreetPause機能を有すること．また，GreetPauseの時間パラメータを，アクセス元のIPアドレスに対応して変更する機能を有すること．

1-5-15. 接続時認証について, あらかじめ設定した回数の認証エラーが発生するコネクションがあった場合, 当該セッションを切断し, かつ, あらかじめ設定した時間のあいだ, 同一のIPアドレスもしくは同一のユーザ名による新規接続を受け付けない機能を有すること．

1-5-16. メールの発信数について, 同一の送信元 (アクセス元のIPアドレスとEnvelopeFromアドレスの組, もしくは, IPアドレスとログインIDの組 で判断する) から, あらかじめ設定した時間以内にあらかじめ設定した数以上のメールを送信しようとした場合, あらかじめ設定した時間のあいだ, メールの発信を禁止する機能を有すること．

1-5-17. 利用者毎に，送信元IPアドレスおよび送信元メールアドレスによる受信拒否設定機能を有すること．

1-5-18. 本システムを通過する全てのメールに対して，ウィルス対策を行う機能を有すること．
★ 本対策機能によりウィルス付きと判断されたメールを，一定期間で自動的に削除する機能を有する場合は, 加点として評価する．

1-5-19. 本システムを通過する全てのメールに対して，SPAMメール対策を行う機能を有すること．ただし，本対策機能によりSPAMと判断されたメールの隔離は，個人ごとに利用者自身が利用の可否を設定する機能を有し，隔離したメールは一定期間で自動的に削除する機能を有し，かつ，削除される前のメールは利用者自身の権限で通常スプールに復活させる機能を有すること．

1-5-20. 利用者毎のメールスプール領域は，ホームディレクトリのクォータ設定と，メールスプールのクォータ設定を独立して設定する機能を有すること．また，クォータ値

が事前に設定した危険水域を越える場合と，限界値に到達した場合に外部に通知する機能を有すること．
★ ホームディレクトリのクォータ設定とメールスプールのクォータ設定を総和として設定する機能を有する場合は，加点として評価する．

1-5-21. CLI を用いて，メールスプール用のクォータ設定を利用者毎に設定する機能を有すること．

1-5-22. 本メールサーバに到着した同一メールドメイン宛の同報メールについて，メールスプール用ディスク容量の重複利用を避ける機能を有すること．

1-5-23.
★ メールの発信時に，予め指定されたサイズを超える添付ファイルが含まれるメールを，ワンタイムパスワードで保護された Web アクセス可能な領域に分離し，送信先に，自動的にアクセス用のワンタイムパスワードを通知する機能を有する場合は，加点として評価する．なお，分離したファイルは一定期間で削除する機能を有すること．

1-5-24.
★ CLI で，項番 1-5-23 の機能を利用者毎に有効化・無効化を設定・参照する機能を有する場合は，加点として評価する．

1-5-25. Web GUI および CLI で管理でき，Subject にメーリングリスト名と連番を付与する機能を有するメーリングリスト機能を有すること．

1-5-26. メーリングリスト毎に，1.2 節で指定した属性を有するユーザが管理する機能を有すること．

1-5-27. メーリングリストに投稿されたメールをアーカイブする機能を有すること．ただし，アーカイブへのアクセスには，1.2 節の認証システムを用いること．

1-5-28. Web GUI および CLI で，メールの転送設定を確認する機能を有すること．

1-5-29. personID(個人一意識別用 ID) アカウントでの利用が可能であること．

1-5-30. 利用者原簿管理システム上のユーザ属性と同期を行う機能を有すること．

1-5-31. 利用者原簿管理システム上のグループ情報と同期し, 更にそれらのグループを組合わせた派生グループを定義できること．

1-5-32. 認証時に統合認証システムから受信するユーザ属性情報を (統合電子メールシステムにおける) ユーザ属性・所属グループ・システム利用資格に反映させる機能 (または同等機能の実装が可能な開発キット) を有すること．

1-5-33. 現行システムのメールスプール，エイリアス，メールドメインリレーおよびメーリングリスト (58 個, DEEPMail) の移行を行なうこと．

1.6　ファイル共有システム 1 式

1-6-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること.

1-6-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること.

1-6-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること.

1-6-4. アクセスログを サーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること.

1-6-5. 独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしてもサービスが停止しない構成であること.

1-6-6. 参照系サービスを停止せずに保守が可能な構成であること.

1-6-7. 参照系サービスを停止せずにデータのバックアップが可能であること.

1-6-8. データベースを利用するシステムの場合は, アプリケーションサーバとデータベースサーバが独立したサーバインスタンスとして分離されていること.

1-6-9. また, データベースサーバは独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしても編集系サービスが停止しない構成であること.

1-6-10. Web ブラウザを通じて以下の操作が行える機能を有すること.

1-6-10-1. ファイルのアップロード・ダウンロードができること.

1-6-10-2. ファイルに対してタグ付けができること.

1-6-10-3. ファイルのバージョン管理ができること.

1-6-10-4. ドラッグ・アンド・ドロップ操作により複数ファイルを一括アップロードできること.

1-6-10-5. フォルダを用いてファイルの階層化管理ができること.

1-6-10-6. ファイル単位・フォルダ単位でアクセス権限を設定できること.

1-6-10-7. フォルダ単位でのダウンロードができること.

1-6-10-8. アクセス権限として少なくとも閲覧権限と編集権限を設定できること.

1-6-10-9. ファイルに対して日本語および英語での全文検索が行えること．なお, 閲覧権限のないファイルが全文検索の結果に含まれないこと.
★ システムに登録された画像ファイルに OCR 処理を施し, 全文検索を可能とする機能を有する場合は加点として評価する.

1-6-11. 日本語および英語の Web クライアント用操作画面を有すること
★ ファイルの更新状況を利用者に通知する機能を有する場合は加点として評価する
★ システムに登録された PDF ファイルならびに Microsoft Office 形式の文書を Web ブラウザ上でプレビュー表示する機能を有する場合は加点として評価する

1-6-12. 名前に日本語を含むファイル・フォルダに対する表示・編集・検索ならびにダウンロード処理を文字化けを起こさずに行う機能を有すること

1-6-13. 誤削除防止機能 (削除対象のファイルを一時的に不可視状態にし, 復旧可能とする機能) 相当の機能を有すること
★ 削除対象のファイルを一旦ごみ箱フォルダに移動する機能を有する場合は加点として評価する

1-6-14. 一時不可視状態にあるファイルをシステムに残す期間を設定する機能を有すること
★ 上記期間をユーザ自身で設定できる機能を有する場合は加点として評価する

1-6-15. 各ファイルに対する操作を監査ログとして残す機能を有すること.

1-6-16. WebDAV(RFC4918) によるファイルのアップロードとダウンロードをする機能を有すること．ただし，WebDAV の認証には統合認証システムで用意されたファイル共有システム用の LDAP を用いること.
★ 専用のアクセス用クライアントソフトが存在する場合, クライアントソフト専用パスワードを発行する機能を有する場合は加点として評価する

1-6-17. CLI で，以下の操作ができる機能を有すること.

1-6-17-1. クォータ設定の設定と参照

1-6-17-2. グループの追加と削除

1-6-17-3. グループへのユーザの追加と削除

1-6-17-4. ファイル・フォルダ所有者の変更

1-6-18. 統合認証システムと連携した SAML 認証または CAS 認証によるシングルサインオンが可能であること.
★ 学外からのアクセスに対して多要素認証を行う機能を有する場合は加点として評価する

1-6-19. personID(個人一意識別用 ID) アカウントでの利用が可能であること.

1-6-20. 利用者原簿管理システム上のユーザ属性と同期を行う機能を有すること

1-6-21. 利用者原簿管理システム上のグループ情報と同期し, 更にそれらのグループを組合わせた派生グループを定義できること.

1-6-22. 認証時に統合認証システムから受信するユーザ属性情報を (ファイル共有システムにおける) ユーザ属性・所属グループ・システム利用資格に反映させる機能を有すること

1-6-23. (ファイル共有システムにおける) ユーザの所属グループ・システム利用資格に応じたアクセス権限の設定をファイル単位ならびにフォルダ単位で行えること.

1-6-24. 一般ユーザがシステムに登録できるファイルの種類をシステム管理者が制限する機能を有すること

1-6-25. 一般ユーザがシステムに登録できるファイルサイズの上限をシステム管理者が設定できる機能を有すること
★ システムに一度に登録できるファイル数の上限をシステム管理者が設定できる機能を有する場合は加点として評価する

1-6-26. 一般ユーザがシステムに登録できる総データ量の上限をシステム管理者が設定できる機能を有すること
★ フォルダに対して総データ量の上限を設定できる機能を有する場合は加点として評価する
★ パブリッククラウド上のストレージを用いて動的にストレージ容量を拡張する機能を有する場合は加点として評価する

1-6-27. 既設 Fortigate1000C の DLP(Data Leakage Prevention) 機能を用い, 正規表現等のパターン文字列で指定されたキーワードを含むファイルの学外送信を防止するように構成されていること．なお，必要なネットワーク機器の設定は，本学側で実施する.

1-6-28. システムに登録されるファイルに対してウイルススキャンを行う機能を有すること.

1-6-29. ファイルを直接参照するブックマーク可能な URI(以下, 直接参照用 URI) を生成できること. また, 直接参照用 URI へのアクセスに対しユーザ認証を行うこと

1-6-30.
★ 認証を行わずにファイルを直接参照することが可能な公開用 URI を生成する機能を有する場合は加点として評価する．なお, 公開用 URI はファイル名からの推測が困難な規則にしたがって生成されること．また, 一度生成した公開用 URI を無効化する機能を有すること.

1.7 認証付きコンテンツ管理システム 1 式

1-7-1. Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること.

1-7-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること.

1-7-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること.

1-7-4. アクセスログを サーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること.

1-7-5. 独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしてもサービスが停止しない構成であること.

1-7-6. 参照系サービスを停止せずに保守が可能な構成であること.

1-7-7. 参照系サービスを停止せずにコンテンツのバックアップが可能であること.

1-7-8. データベースを利用するシステムの場合は, アプリケーションサーバとデータベースサーバが独立したサーバインスタンスとして分離されていること.

1-7-9. また, データベースサーバは独立した 2 つ以上のサーバインスタンスで構成されており，1 つのインスタンスが停止したとしても編集系サービスが停止しない構成であること.

1-7-10. 調達に含まれる全端末パソコンからの同時の Web ページ閲覧要求に対して，最大 1 分以内での応答性能を有すること.

1-7-11. メニューおよび階層化コンテンツを備えた Web サイトの運営が可能であること.
★ システムに登録された PDF ファイルならびに Microsoft Office 形式の文書を Web ブラウザ上でプレビュー表示する機能を有する場合は加点として評価する

1-7-12. 新着情報を自動的に利用者に表示する機能を有すること.

1-7-13. 検索エンジンに登録可能なサイトマップを生成する機能を有すること

1-7-14. 検索ロボットからのアクセスを許可するコンテンツの範囲を指定する機能を有すること

1-7-15. 入力項目をカスタマイズ可能なオンラインフォームを提供する機能を有すること.

1-7-16. 統合認証システムと連携した SAML 認証または CAS 認証によるシングルサインオンが可能であること.
★ 学外からのアクセスに対して多要素認証を行う機能を有する場合は加点として評価する

1-7-17. 統合認証システムと連携した LDAP による認証が可能であること.

1-7-18. personID(個人一意識別用 ID) アカウントでの利用が可能であること.

1-7-19. 利用者原簿管理システム上のユーザ属性と同期を行う機能を有すること

1-7-20. 利用者原簿管理システム上のグループ情報と同期し, 更にそれらのグループを組合わせた派生グループを定義できること.

1-7-21. 認証時に統合認証システムから受信するユーザ属性情報を (認証付きコンテンツ管理システムにおける) ユーザ属性・所属グループ・システム利用資格に反映させる機能を有すること

1-7-22. (認証付きコンテンツ管理システムにおける) ユーザの所属グループ・システム利用資格に応じたアクセス権限の設定をコンテンツ単位ならびにコンテンツの階層単位で行えること.

1-7-23. また, アクセス権限として少なくとも閲覧権限と編集権限を設定できること
★ コンテンツの更新権限と削除権限を分けて管理する機能を有する場合は加点として評価する

1-7-24. 閲覧権限のあるコンテンツ階層だけがメニューに表示されること.

1-7-25. Web ブラウザ上で言語選択操作を行うことで日英コンテンツの切替が可能であること.

1-7-26. 日英コンテンツの紐付けが可能であること.

1-7-27. アクセスするデバイスの解像度に応じて表示レイアウトを自動調整する機能を有すること.

1-7-28. ページテンプレートの作成機能があること.

1-7-29. ユーザがページレイアウトを複数候補の中から選択できること.

1-7-30. ユーザが登録する HTML コンテンツに対し，クロスサイトスクリプティング攻撃を防止するためのサニタイジング処理を行うか，または利用可能な HTML タグを制限する機能を有すること

1-7-31. 各ページに対し, 複数のファイルをコンテンツとして添付できること.
★ システムに登録されるファイルおよびコンテンツに対してウイルススキャンを行う機能を有する場合は加点として評価する

1-7-32. Web ブラウザ上のドラッグ・アンド・ドロップ操作により複数ファイルを一括アップロードする機能を有すること

1-7-33. システムに登録できるファイルの拡張子をシステム管理者が制限する機能を有すること

1-7-34. システムに登録できるファイルサイズの上限をシステム管理者が設定できる機能を有すること
★ システムに一度に登録できるファイル数の上限をシステム管理者が設定できる機能を有する場合は加点として評価する

1-7-35. コンテンツを階層化して管理できること.

1-7-36. コンテンツに対してタグ付けができること.

1-7-37. コンテンツのバージョン管理ができること.
★ 編集ワークフロー機能を有する場合は加点として評価する

1-7-38. コンテンツに対して日本語および英語での全文検索が行えること．なお, 閲覧権限のないコンテンツが全文検索の結果に含まれないこと．
★ システムに登録された画像ファイルに OCR 処理を施し, 全文検索を可能とする機能を有する場合は加点として評価する

1-7-39. 既設 Fortigate1000C の DLP(Data Leakage Prevention) 機能を用い, 正規表現等のパターン文字列で指定されたキーワードを含むファイルの学外送信を防止するように構成されていること．なお，必要なネットワーク機器の設定は，本学側で実施する．

1-7-40. 以下の要件を満たすマルチテナント運用が可能な機能を有すること

1-7-40-1. テナント毎に異なったサイトのテーマ (スタイルシート, ロゴ, ページレイアウトなど) を利用できること．

1-7-40-2. テナント毎に固有のサーバ URI を利用できること．

1-7-40-3. テナントを利用できるユーザをユーザ属性・グループ情報に基づいて制限できること．

1-7-40-4. テンプレートサイトを用いてテナントを初期化する機能を有すること．

1-7-40-5. テナント単位でのデータのバックアップ・リストアが可能なこと．

1.8 セキュリティ対策ソフトウェアシステム 1 式

1-8-1. Microsoft 社 Windows Server 2012 相当以上，または， Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．

1-8-2. SSHv2 による遠隔ログイン機能を有すること．ただし，Windows 系の OS での提案の場合は，通信路が 128bit 以上の暗号化鍵で暗号化されたリモートデスクトップサービスで代替しても良い．なお，予め指定された管理者ユーザのみログインできる機能を有すること．

1-8-3. 本対策ソフトウェアのクライアントアプリケーションのパターン定義ファイルを提供し，各クライアントの更新状況を参照する機能を有すること．
★ 学外に持ち出しているクライアントを識別してパターン定義ファイルを提供する機能を有する場合は，加点として評価する．

1-8-4. 本対策ソフトウェアのクライアントアプリケーションのインストール数を数える機能を有すること．

1-8-5. 少なくとも 5000 台のクライアントにインストールするライセンスを有すること．
★ 本学の保有するすべてのクライアントにインストールするライセンスを有する場合は, 加点として評価する．

1-8-6. 対応するクライアントは，少なくとも以下に挙げる OS であり，本システム上で必要となるサーバおよび端末パソコンを含む本学構成員が利用する備品パソコンにインストールしてセキュリティ対策を行う機能を有すること．

- Windows 7/8/8.1/10 (32bit/64bit 版)
- MacOS X 10.9,10.10,10.11 および macOS 10.12
- Red Hat Enterprise Linux
- Ubuntu Linux

★ また，本学構成員が大学に持ち込むパソコンにインストール可能なホームユースライセンスを有する場合は，加点として評価する．

1-8-7. クライアントに含まれるアンチウィルスエンジンは，1.5 節の電子メールシステムに含まれるアンチウィルス機能のエンジンと異なるベンダーのものであること．

1-8-8. ウィルスパターンの更新状況をサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1.9 ライセンス管理システム 1 式

本システムは, 提案に含まれるライセンス制約条件を満たすために非仮想化サーバ装置で実現しても良い. その場合, 2.3 節の仕様を満たした装置であり, 本節記載の性能要件をすべて満たすように構成すること．

1-9-1. Microsoft 社 Windows Server 2012 相当以上，または， Red Hat Enterprise Linux Server 7.2 相当以上のオペレーティングシステム上で稼働するシステムであること．

1-9-2. SSHv2 による遠隔ログイン機能を有すること．なお，予め指定された管理者ユーザのみログインできる機能を有すること．ただし，Windows 系の OS での提案の場合は，通信路が 128bit 以上の暗号化鍵で暗号化されたリモートデスクトップサービスで代替しても良い．

1-9-3. IPv4 と IPv6 トランスポートのいずれからのアクセスであっても接続を受け付け，かつ，アクセス制限設定する機能を有すること．

1-9-4. ライセンス使用ログをサーバ監視システムに専用の VLAN もしくは SSL 通信相当以上と判断される方式で送信する機能を有すること．

1-9-5. サイトライセンス (Mathematica, PTC/Creo, IBM CATIA) について，ライセンス使用数，ライセンス使用クライアント，ライセンス毎の利用開始時刻および終了時刻を記録する機能を有すること．なお，PTC/Creo, Pro/ENGINEER および IBM CATIA のライセンスは本学側で調達したものを適用する．

1-9-6. 本調達で使用する RedHat Enterprise Linux を使用する場合,
★ サブスクリプション管理に RedHat Satellite 相当以上と判断される管理機能を有する場合は加点として評価する．