メールセキュリティ強化対応
業務委託仕様書

2020 年 11 月 18 日

公立大学法人　横浜市立大学

1. 導入の方針等

1.1 導入の趣旨

公立大学法人 横浜市立大学(以下、本学)は、国際教養学部、国際商学部、理学部、データサイエンス学部、医学部の 5 学部、都市社会文化研究科、国際マネジメント研究科、生命ナノシステム科学研究科、生命医科学研究科、医学研究科の 5 研究科を横浜市内 4 キャンパスに展開し、附属 2 病院を擁する総合大学である。

本学は、「国際都市横浜と共に歩み、教育・研究・医療分野をリードする役割を果たすことをその使命とし、社会の発展に寄与する市民の誇りとなる大学を目指す。」のミッションのもと、多角的に物事を考える力を養う教養と特色ある高い専門性を兼ね備えた、豊かな人間力を有する人材を育成することを教育ポリシーとしている。

大学の教育ポリシーに基づいた教育・研究・医療を提供するためには、より「利便性」「安全性」「可用性」「運用性」の高いシステムが必須である。大学の業務を行なうにあたって、電子メールを活用してやり取りが多くなってきているが、容易に遅れる半面、送付先を誤って情報漏洩事故が生じることがあり、現実、本学においても事案が生じている。特に業務で送付するファイルは個人情報や機密情報を含んでいるものもあり、事故が生じた場合に影響が大きいので、添付ファイル付きのメールの対策を強化する必要がある。また、外部から送信されるメールには不正な挙動をするファイルが添付されているものがあり、学内の情報を守るためこうしたファイルの侵入を抑止する対策が必要になっている。そこで、現在本学で提供しているメールサービスにおいて、メールによる外部からの攻撃に備える入口対策、情報漏洩を未然に防止する出口対策を実現するメールセキュリティ対策システムを構築する。

1.2 メールセキュリティ対策システムの構成

今回更新対象とするメールセキュリティ対策システムの範囲を以下のように定義する。
各システムの構成物については「3 メールセキュリティ対策システムの要求仕様」に詳しく記述する。

表 1 メールセキュリティ対策システムの構成

メールセキュリティ対策システム	メールセキュリティ対策サーバ、ファイル配信サーバの総称。
メールセキュリティ対策サーバ	基本的なメールセキュリティ対策サービスを提供するためのサーバ。 以下のサービスを含む。 ・入り口対策（攻撃対策）機能 ・出口対策（誤送信防止）機能 ・その他監査等に関わる機能
ファイル配信サーバ	ファイルをメールへの添付によらずに配信するためのサーバ。

※仕様を満たしたものであれば、上記の区分によるサーバ構成でなくてもよい

1.3 調達の範囲

今回の調達では要求仕様に示したメールセキュリティ対策システムのほか、以下の業務の履行を含める。

詳細なスケジュールは契約後、大学と協議のうえ決定するが、システムの構築は令和3年6月30日までに行い、運用保守は構築完了から令和4年3月31日までの間実施することを想定し、次の事項を実施すること。

(1) システムの構築
- ア システム構築から運用開始(サービスイン)までのプロジェクトマネジメント業務
- イ 必要なハードウェア、ソフトウェア、その他機材の提供
- ウ 機器の設置、設定、動作テスト
- エ ソフトウェアのインストール
- オ 必要に応じてネットワーク設計・設定変更、配線工事、電源工事、機器取り付け工事

カ 利用者用操作マニュアル、システム管理者用運用マニュアル作成
キ 本学管理者への操作説明
ク 本学利用者への操作説明

(2) システムの運用保守
ア 導入したシステムに対する障害対応
イ 運用開始後に生じた導入ソフトウエアの軽微な設定変更
ウ 導入ソフトウエアの修正モジュールのサーバへの適用
エ 本学管理者からの導入ソフトウエアの利用に関する問い合わせ
オ 導入ソフトウエアの履行期間中の継続利用料
カ 機器を増設した場合の履行期間中の機器保守

1.4 構築プロジェクトの要求工程

以下のプロセス、もしくはそれに該当するプロセスを実施する。

(1) 概要設計
ア システム全体設計
イ システム基盤基本設計
ウ 既存システム・ネットワーク基本設計
エ アプリケーション基本設計

(2) 詳細設計
ア システム基盤詳細設計
イ 既存システム・ネットワーク基本設計
ウ アプリケーション詳細設計

(3) 導入スケジュール調整
ア プロジェクト実施計画の作成
イ WBS(Work Breakdown Structure:作業分解構成図)の作成

(4) 導入およびテスト
ア アプリケーション作成
イ 単体テスト
ウ 結合テスト
エ システム基盤への組込・整備
オ システムテスト(システム単体、システム間接続、外部機器との接続等)
カ 運用・シナリオテスト
キ 受入テスト(本学職員によるテスト)

(5) システム導入および移行
ア アプリケーション導入
イ システム管理者向け研修
ウ ユーザ研修

1.5 成果物に関する事項

(1) 成果物の作成においては、様式、体裁、装丁、語句の表記方法等の統一を図るとともに、その質を監査する為の要員を配置し、十分な品質管理を行うこと。

(2) 成果物のデータに設定されるタイトル、作成者名、会社名といった属性情報については、あらかじめ案を用意したうえで本学に確認すること。

(3) 成果物のうち、本学が要望する機能要件を実現するために、受託者が個別に対応した部分を含む機能の実現に関する情報が記載されたシステム設計書、データベース定義書等については、個別で対応した箇所が識別できるような措置を講じておくとともに、その個別対応に及んだ背景やシステム機能実装上の制約事項等、ソフトウェア保守の際に重要となる関連情報について追記・明示して納品すること。

(4) 文書等の成果物を電子ファイルで納入する場合、当該ファイルや格納ディレクトリ（フォルダ）の作成にあたって、以下の基準を順守すること。

ア 電子メールにファイルを添付する場合があることを念頭において、ファイル名等に半角カナ文字の他、①、Ⅰ、㈱等の機種依存文字を含めないこと。

イ ファイル名等に半角または全角の空白文字をいれないこと。

ウ ファイル名等の命名はソート順を意識すること。

(5) 導入に必要な機器及びソフトウェアの納入において、製品に添付されるマニュアルや CD-ROM、保証書等の同梱品の扱いについては以下のとおり作業を行うこと。

ア インストールキーや製品シリアル番号等、マニュアルや CD-ROM に製品個々の独立性を表意する情報の印刷・刻印等がなされている場合は、インデクスシールを貼付してまとめること。特に、機器管理番号等との関連を明記した一覧表のファイルを必ず作成し、どの製品に付随したマニュアル、CD-ROM かどうかわかるようにしておくこと。

イ 前項（b）とは異なり、製品個々による独立性を表意する情報が添付されていないマニュアルや CD-ROM については、同種類を一様にまとめて整理するか、本学と協議のうえで廃棄可能なものは一定部数のみ保存し、他を廃棄処分とするなど、適切な措置を講じること。

ウ ハードウェア及びソフトウェア製品の開梱に伴う廃棄物が発生する場合は、受託者の責任において処分することとし、業務履行場所に廃棄物をそのまま放置しないこと。

エ 設計に係る成果物は次に掲げるドキュメントを基本とし、詳細は納品前に本学と協議すること。

(ア) 開発工程表及び開発体制表
(イ) システム概要図（各システム・サーバの関連・全体構成を図示）
(ウ) すべてのハードウェアの設置場所が確認できる配置図面（ラックマウント図、教育実習室端末の設置図を含む）
(エ) システム設計書（機能、定義、インタフェース、データベース、モジュール、その他カスタマイズ部分も含む設計に係る事項の記載）
(オ) ハードウェア設計書（仕様、構成、設定、デフォルト値とチューニング後の初期値、その他設計に係る事項の記載を含む）
(カ) ネットワーク設計書（構成、設定値一覧、パラメータシート、VLAN 割り当て、ポート接続状況、その他設計に係る事項を含む）
(キ) IPアドレス管理表（NW 機器、サーバ類、クライアント端末類の一覧）
(ク) ソフトウェアのライセンス一覧（有償・無償・ライセンス数の判別が可能であること）
(ケ) テスト実施計画書
(コ) 本番稼働計画書
(サ) 研修実施計画書
(シ) 研修で使用した全ての資料
(ス) インストール手順書（サーバ、端末等全て）
(セ) 各種検討報告書
(ソ) 協議に関する記録等
(タ) 各システム及び機器間の接続要件仕様書
(チ) その他、システム管理上必要と考えられるものについては、本学と別途協議すること。
(ツ) 運用手順書（サーバ管理手順、運用スケジュール、メンテナンス手順、バッチ処理手順、他システムとの相互依存、連絡体制図、その他運用上必要な手順等を含む）
(テ) 保守関連手順書
(ト) 障害時の事故管理等手順書（障害時の対応、連絡体制、復旧方法、動作確認方法等含む）
(ナ) 機器管理番号を含むハードウェア一覧表、構成図等
(ニ) 利用者向け操作マニュアル
(ヌ) システム運用マニュアル（通常時、イレギュラー対応時、管理機能と操作手順、権限設定方法等含む）
(ネ) その他、システム管理上必要と考えられるものについては、本学と別途協議すること。

2. システム全般に関わる基本要求

本システムの更新にあたり、基本的な要求事項を以下に示す。

2.1 システムの利便性・操作性・運用性

(1) 極力一般的に入手できるハードウェア、ソフトウェアで構成し、学生や教職員が直接使用するものについては、使用・運用において特別な知識やスキルを必要としないこと。使用において、特別な操作が必要な場合は、GUI ベースで操作できること。

(2) 標準化された規格を採用すること。ただし、将来性のある最新技術も、信頼性、保守性、経済性を確認できれば積極的に導入するので、採用する場合は事前に本学と協議すること。

(3) レスポンスや応答時間がユーザにとってストレスのない範囲であること。そのための目標とするレスポンスを設定し、これを実現するためのシステムのチューニング（ネットワークの整備も含む）を施すこと。また、データの増加などによりシステム性能が低下しないよう考慮されていること。

(4) 障害や不具合により運用継続ができなくなることでシステム全体の可用性に致命的な影響を与える主要部分については冗長化し、故障してもサービスを停止しない構成をとすること。

(5) アプリケーションソフトウェア、パッケージソフトウェアについては本学の指定がない限りは安定している最新のバージョンで導入すること。

2.2 システムの拡張性・柔軟性

(1) システムを構成するソフトウェア、ハードウェア（CPU、メモリ、ストレージ等）について、十分な拡張性、柔軟性を有すること。

(2) 利用者やデータの増加等に対応できるよう、情報システム資源はスケーラブルな構成とし、システムの停止を必要とせずに拡張できるよう考慮すること。本学仮想化基盤サーバの利用もしくは新規基盤の構成とする。

2.3 システムの信頼性・可用性

(1) 設備の長時間にわたる停電などの場合を除き、システムは 24 時間 365 日の安定した連続運用が可能であること。

(2) ネットワーク障害、システム障害などの各種障害が発生した際に、復旧のための原因特定が可能となるよう適切なログの採取を考慮したシステムとすること。

(3) 定期的なバックアップと、本学が承認した障害時のリカバリ手順を明確にすること。

(4) リカバリ手順や所要時間は本学と協議し承認したものとすること。
サーバ機器およびネットワーク機器に対しては、常時監視を行い異常時にはシステム管理者等へ警告を発する仕組みを考慮すること。

2.4 システムのセキュリティ

(1) 機密情報や個人情報の保護のため、使いやすさを維持しつつ適切なアクセス制御ができる仕組みを備えていること。

(2) ユーザ管理など重要なデータへのアクセス、及び、学外からのリモートアクセスについては、アクセスした利用者、アクセス先の情報、時間、端末、件数等を特定できる履歴（アクセスログ）を蓄積し、その解析をシステム管理者が随時かつ容易に行えること。

(3) ログの保存期間は原則 1 年以上とし、システムごとに本学と検討のうえ決定すること。

2.5 システム容量および性能

(1) 容量、性能は、年間増加率を考慮し、最低 5 年間は機器の増設なしで運用できるよう考慮すること。

(2) システムごとにあらかじめ設定した閾値を超えた場合に、自動的にシステム管理者に通知すること。

(3) リソースの利用状況を常時確認できるようにし、長期未使用者や退職者等のリソースを容易に再使用できるようにすること。

2.6 設置

(1) 設置場所

メールセキュリティ対策システムを構成するサーバは、原則としてデータセンター内既設仮想化基盤サーバに構築するが、リソースが不足する又は仮想化基盤で対応不能の場合は、本学と協議のうえ、仮想化基盤の増設又は物理サーバによる構築も可能とする。ただし、機器はデータセンター内に設置とするものとし、設置する機器、データセンターへの設置や調整に係る費用は全て本業務に含むこととする。

(2) 電源設備

ア 新たに装置を設置する場合、原則、最寄りの分電盤より分岐して電源をとるなどして対処すること。また、これと異なる電圧、周波数の電源で稼働する装置は、電圧変換、周波数変換等の設備を用意すること。

イ 設置する機器が設置済みの空調設備以上の冷房能力を必要とする場合、また特殊な冷却設備が必要な場合はその設備を用意すること。

ウ 電源コンセントの形状により変換アダプタが必要な場合は用意すること。

(3) 電源管理

ア データセンター以外に設置するサーバ類には、停電時に安全なシャットダウンプロセスで停止できるよう無停電電源装置(UPS)を提供すること。

イ UPS は停電発生時、5 分間の待機時間を経てから、システムが正常に終了できる電源容量を確保すること。

(4) 搬入・据付・配線・調整

ア 物品の搬入・据付・配線・調整等に関しては、作業開始前の本学が求める期限までに、搬入経路や配管の確認・必要な車両等の通知・駐車場利用時間の明示などを行い、事前に調整して作業方法を決定し、その内容に従って実施すること。

イ 導入工程表を作成し、本学の承認を得ること。なお、工程表には工程名称、期間、目的、定例報告予定日、各システムの導入時期、管理者研修、ユーザ研修などのマイルストーンを明記すること。

ウ 本学が用意した一次側電源設備から各機器への配線も行うこと。

エ 既設システムやネットワークとの接続について障害が発生した場合は原因の分析を行い、起因する障害については対処すること。

オ 本学の施設内に設置する全ての機器について、盗難防止措置及び安全のための転倒防止措置を講じること。

カ 構築業者は導入計画書に、構築から移行時のラック搭載計画を記載すること。

キ 導入するシステムの動作に必要なディスプレイ、キーボード及び切替機を提供すること。

ク その他設置に必要なケーブル類は全て提供すること。設置されるハードウェアは、機器管理番号や IP アドレス、サブネットマスク、VLAN の ID 等のネットワーク定義情報を明示することとし、原則として着脱可能なマグネットシールやタグ等を貼付すること。特に、これらの準備及び貼付にかかる一切の費用は受託者の負担とする。なお、明示する情報の内容については、本学と別途協議すること。

(5) バックアップ

ア 機器故障や誤操作によるデータの消失回避のため、各サーバの復旧用イメージ及びデータのバックアップを取得すること。保存先はデータセンター内の別媒体とすること。

イ 導入サーバについて、2世代のフルバックアップを取得すること。

2.7 導入・テスト・研修

(1) プロジェクト体制

ア 導入・構築を行うプロジェクトマネージャが、下記のいずれかの資格または相応する能力を保有していること。

(ア) 情報処理推進機構実施の情報処理技術者試験「プロジェクトマネージャ」

（イ） 米国プロジェクトマネジメント協会（PMI）本部認定「PMP 国際資格」

イ 各作業担当者はメールセキュリティ対策システムの導入に当たり、本学の環境を十分把握したうえで、業務を行うこと。

ウ 設計・構築要員とテスト要員は、各々別の人物を充てるなどにより品質を確保すること。

エ システムの構築及び付随する業務の遂行にあたっては、作業分担、編成時期等を明確にした組織（要員）管理計画書を作成すること。

オ 分担した作業ごとにプロジェクトチームを編成し進捗管理を行うこと。また、マルチベンダ構成によるチームを編成する際には、受託者が総責任者となる組織（要員）管理体制とすること。

カ プロジェクトの体制を変更する場合には、その事由と新体制について事前に本学に説明し、協議したうえで実行すること。

キ 作業担当者を交代する場合は、業務一切の引き継ぎを確実に行い、それにより業務に支障が生じないようにすること。

ク 各作業担当者には個人情報の取り扱いと大学内のルール及び倫理・道徳・社会常識について指導をすること。

ケ 定期的（月次・週次）に進捗報告会議を実施し、スケジュール上の課題が発生した場合は本学と共有、協議のうえ解決すること。また、その会議で共有する資料は、その内容について受託者の担当者間で会議の場で齟齬や認識の相違が生じないよう、受託者内部で十分なレビューや査閲を行ったうえで、会議前日までにはそれらのデータを本学に送付すること。

コ 進捗報告会議にはプロジェクトマネージャが必ず参加すること。なお、会議の形態は WEB 会議でも構わないが、少なくとも月に 1 度は対面にて会議を実施すること。

サ 各プロセスの終了時には、受託者内部で十分なレビューを実施し、そのレビュー結果を本学に提示すること。なお、本学が不要と判断しない限りは、原則としてプロセスごとに本学と共同レビューを実施し、承認を得ること。

シ 進捗会議、レビュー会議における議事録は受託者が作成すること。

(2) テスト

ア 全てのテストにおいて、テスト仕様書及び結果報告書を提示し承認を得ること。テスト項目・パターンに漏れがないか事前に本学に確認すること。

イ 単体・結合テストは受託者保有の機器、製品を使用して実施すること。

ウ システムテストは、本番機器の導入後であれば、実機を使用すること。また、既存システムの環境を用いてテストを実施する場合には、事前に本学と協議し、その指示に従うこと。

エ 運用・シナリオテストは受託者が事前に本学の運用について詳細にヒアリングしたうえで、テストパターン（シナリオ）を用意すること。

オ 受入テストは本学が実施主体となり行うが、受託者は必要な設定等の作業支援を行うこと。

カ 受入テストの実施にあたって、運用・シナリオテストで使用したテスト仕様書、テストデータ、テストシナリオを全て本学に提示すること。

キ 受入テストに使用するテストデータについては、受託者が作成すること。

ク 受入テスト期間中は、本学職員からの問合せを受けられるよう、受託者は立ち会いをすること。

ケ 受入テスト後の修正にあたってはデグレードしないように細心の注意を払うこと。

コ テスト時に使用した不要なデータ、ユーザ ID、プロセス、サービスはテスト完了時にシステムから完全に削除すること。

サ 冗長構成によるシステム切り替え等については実機によるテストを確実に実施し、想定した通りの暫定運用、復旧の手順を確認すること。

シ 本番環境の動作制限や外部に影響するようなテストは、少なくとも実施の 1 ヵ月以上前にその内容やスケジュール等の概要を本学に提示して調整を図ること。

(3) 導入

ア ネットワークやサービスの停止および騒音を伴う作業については、原則として土日、夜間に実施することを前提とし、詳細は本学と別途調整すること。

イ 各作業担当者は自らの所属等を証明するものを常時携帯するとともに、一般に目視できる位置に名札等を着用すること。

ウ　各作業担当者が本学内各室に立ち入って作業を行う際は、原則として、事前に本学の許可を得たうえで作業を進めること。

エ　本業務に関わる機密事項や本学で知り得た学生情報、職員情報、患者情報等を取り扱うにあたり、受託者は、本業務に携わる者以外にこれら一切の情報が漏洩しないよう、十分に配慮すること。

(4) 研修

ア　メールセキュリティ対策システムの導入にあたり、次の研修を行うこと。

(ア) ユーザ(教職員)向け研修

(イ) システム管理者向け研修

イ　講師および研修資料の準備をすること。研修資料は事前に作成し、本学の承認を得ること。

ウ　研修に参加できないユーザ向けに、メールセキュリティ対策システムの機能と利用方法を十分に理解できる動画、または資料を用意し、本学の Web サイトで公開できるようにすること。

エ　研修の際には、実際の運用に即したデータを準備すること。

オ　1 日午前、午後に分けて各 1 時間、もしくは 2 日間で計 2 回各 1 時間、リモートのユーザ向け研修を実施すること。

カ　1 日午前または午後に1回、リモートの管理者向け研修を実施すること。

2.8　運用保守について

(1) システム運用管理委託範囲

システム構築完了から本委託契約の履行期限までの1．3(2)に記述する事項

(2) 保守体制

ア　メールセキュリティ対策システムに精通するものを充てるなど迅速に対応できるようにすること

イ　作業実施前及び完了時に作業項目、結果を本学の管理者に報告すること。

ウ　保守サポート体制の範囲は、今回導入した製品を範囲とするが、必要に応じて関連部分も調査し、情報の提供・支援が行えること。

エ　既設ネットワークとの接続においてメールセキュリティ対策システムと関連して障害が発生した場合、原因の分析を早急に行い、受託者の作業に起因する障害については迅速かつ真摯に対処すること。

オ　保守対応時間は原則として祝日、年末年始などを除き月曜日から金曜日の 8 時 30 分から 17 時 30 分までとする。ただし、週末や祝日などに行う作業や緊急性の高いメンテナンスを行う場合で教職員や学生に影響を生じさせない必要がある作業については、別途本学と協議のうえ、それ以外の時間でも対応すること。

カ　支援体制図・人員体制表を提出し、本学へのサポート体制を明確にすること。

キ　保守サポートの作業内容について詳細は契約後に本学と協議のうえ決定する。

2.9　契約不適合責任期間及び著作権の取扱いについて

(1)　本件の履行の目的物に関する契約不適合責任期間は、本学委託契約約款に準ずることとする。

(2)　業務アプリケーションの稼働に必要となる各種ソフトウェア及びハードウェアの稼働については、それらの製造者や販売者となっているかどうかを問わず、本システム稼働前に公表されていない他社製品における根本的なバグ等不具合を除き、受託者がトータルシステムとして最終的な稼働の責任を負うこと。

(3)　今回調達するシステムで採用する、あるいは、構築作業に関連して利用する、OS・ミドルウェア・フリーソフト(ソフトウェア)等について、ベンダが既に公表していた不具合等のリリースノートを確認せず、必要な対処を怠ったことによって生じた障害や不具合の責任については、受託者が負うこと。

(4)　受託者の関連会社または協力会社が開発作業に参画する体制を採用することも可能とするが、その場合は受託者が責任をもって契約上及び実行上の品質確保要件を盛り込み、それらに従って関連会社・協力会社の監督をすること。また、それら関連会社・協力会社に対し、本章等の業務遂行にかかる要件の周知徹底を十分に図ること。

3. メールセキュリティ対策システムの要求仕様

メールセキュリティ対策システムを構成する機器およびシステムの要件を以降に示す。原則、記載されている構成で実現することを想定しているが、他の構成や機器を用いてより効率的に導入ができると考える場合や、システムの要件を満たすために必要と考える機器や数量の増減がある場合は、本学と協議したうえで構築すること。

本調達に含まれない既設のサーバ・NW 機器の設定変更がやむなく必要な場合、受託者がその作業を請け負うこと。

既設のケーブルや取り付け器具等も支障がなければ利用してよいが、新たにケーブル敷設工事等が必要な場合は、本調達に含めること。

3.1 メールセキュリティ対策サーバ

本学の情報セキュリティを強化させることを目的として、原則既設仮想化基盤サーバ上にソフトウェアを構築すること。

要求事項	要求仕様
数量・ ハードウェア	メールセキュリティ対策基本ソフトウェアを動作させるためのサーバ。 冗長性を考慮した構成にすること。 以下のソフトウェア及び制約条件を満たすリソースを用意すること。
ソフトウェア 及び 制約条件	(1) 入り口対策(攻撃対策)機能 ア SPF、Sender-ID、DKIMの方式を利用し、認証結果や添付ファイルの有無などに応じて、配送や注意喚起文言の挿入、破棄などを行うことができること。 イ 受信した実績のない外部アドレスからメールを受信した場合にはじめて受信するアドレスであることをメール本文中に挿入し、注意喚起を行うことができること。 ウ 返信等の送信した実績のない外部アドレスから添付ファイル付きのメールを受信した場合に、返信等の送信した実績のないアドレスであることをメール本文中に挿入し注意喚起を行うことができること。 エ 特定のIPアドレスやドメインメールアドレスから送信されるメールは、迷惑メールに分類されないようにホワイトリストとして管理できること。尚、リストは5,000件の登録ができること。また、ユーザごとにホワイトリストを分割管理できること。 オ 送信メールサーバから受信メールサーバまでのメールの配送経路の通信を暗号化できること。 カ 相手サーバがTLSをサポートしていない場合には平文で送信することができること。さらに、相手サーバがTLSサポートを応答したにもかかわらず、相手の暗号スイートが古い、証明書が失効している、TLSのバージョンが古い場合にも、平文で配送し、再送の繰り返しや配送不能とならないようにすること。 ク 特定のサーバ間の通信は暗号化を強制できること。 ケ 社外からの特定の拡張子、ファイル種別が添付されたメールの受信を制限することができること。 コ フリーメールから送信されたメールでメールアドレスのフレーズ部分の偽装対策として、Subjectに### freemail ### のような文字列を挿入できること。 サ フリーアドレスからのメールなど特定のフィルタリング条件に合致するメールについて、添付ファイルをPDF化することでマクロやスクリプトを除去し、攻撃を無効化できること。 (2) 出口対策(誤送信防止)機能 ア ToまたはCcに10件以上の宛先が含まれる場合、Bccに変換して送信するこ

	とでメール送信先間での送信先メールアドレスの漏洩を防ぐことができること。 イ 過去に送受信履歴のあるアドレスに送信するメールに、PW付きZIPで保護されていないファイルが添付された場合、名簿などの個人情報ファイルが含まれているかを判定できること。 ウ イで個人情報ファイルが含有していると判定した場合には、メールの送信を停止できること。 エ イで個人情報ファイルが含有していると判定した場合には、本文に以下のような内容を記載し、添付ファイルをシステム側でZIP暗号化し送信者に自動返送できること。 (ア) ZIPのPW (イ) 個人情報が含まれると判定され、PW保護がないために差し戻された旨を伝える文言 (ウ) ZIPを添付して改めて送信するよう指示する文言 (エ) ZIPのPWは、「相手からの返信により宛先に間違いないことを確認後」、または「メール以外の手段を使って」相手に連絡するよう指示する文言 オ 過去に送受信履歴のないアドレスに、PW付きZIPで保護されていない添付ファイルが付与されているか検知ができること。 カ オで検知がされた場合には、メールの送信を停止できること。 キ オで検知がされた場合には、本文に以下のような内容を記載し、添付ファイルをシステム側でZIP暗号化し送信者に自動返送できること。 (ア) ZIPのPW (イ) 送信先のアドレスのリストと宛先に間違いがないか確認を促す文言 (ウ) ZIPを添付して改めて送信するよう指示する文言 (エ) ZIPのPWは、「相手からの返信により宛先に間違いないことを確認後」、または「メール以外の手段を使って」相手に連絡するよう指示する文言 (3) 性能要件 ア 入口対策及び出口対策を考慮したうえで、次のスループットを満たすこと。 (ア) PDF変換:メールサイズ150KBで平均処理通数80通/sec (イ) その他機能:メールサイズ150KBで平均処理通数3000通/sec (4) その他機能 ア ウイルス検知や承認依頼メールなどの通知メールでは、日本語・英語やその他言語を併記することができるなど自由に文面を定義できること。 イ ログによる監査が行えるよう、メールタイトル、添付ファイル名、添付ファイルサイズのログが出力できること。 ウ 組み込んだルールにどの程度のメール件数が該当したかの有効性確認ができること。特定のフィルタリング事象発生時に個別のタグをつけたログを残すことで、監査を容易に実施できること。 エ 新たに見つかったウイルスのパターンファイルの対応前に過去に内部に配送されていないかを確認できること。(添付ファイルのハッシュコードをログに出力しておくことなどにより、確認できる手段を提供すること。)
その他	(1) 2.システム全般に関わる基本要求に準拠すること。

3.2　ファイル配信サーバ

メールセキュリティ強化の一環として、原則既設仮想化基盤サーバ上にメールの添付ファイルを分離し配信・公開するソフトウェアを構築すること。

要求事項	要求仕様
数量・ ハードウェア	ファイル配信用のソフトウェアを動作させるためのサーバ。 ストア領域はユーザに必要な分を確保すること。 以下のソフトウェア及び制約条件を満たすリソースを用意すること。
ソフトウェア 及び 制約条件	(1)　WebDAVプロトコルに準拠した機能を有し、WebサーバにはTomcatを使用していること。 (2)　利用者がWebブラウザでファイルの操作を行えるWebインタフェースを有すること。Webブラウザは Internet Explorer、Microsoft Edge、Google Chrome、Firefox、Safariの最新版で動作すること。証明書ありのSSL通信に対応すること。 (3)　Webインタフェースのロゴマークや色を本学の仕様に変更できること。 (4)　iOS, AndroidOSスマートフォンからのファイル・フォルダ操作を可能とする(公式アプリがAppStore、GooglePlayにて無償提供されている)こと。 (5)　個人フォルダの他、複数のグループフォルダが設定できること。また、各グループフォルダを利用できるユーザをグループ毎に設定できること。 (6)　ユーザアクセスは7,000ユーザ利用できること。 (7)　個人フォルダ毎にシステムで保存容量の制限ができること。 (8)　ファイル保存期間は、一律で「ファイル保存開始日より○日まで」のように日単位での設定がシステムでできること。最大30日間保存すること。 (9)　添付ファイル付きメールをサーバに送付することで、メール本文より添付ファイルを分離してサーバ上へ保管し、メール本文にダウンロードアドレスを挿入可能な機能を有すること。 (10) ダウンロードアドレスに自動的にパスワードを設定することが可能で、パスワードをメール送信者へ通知する機能を有すること。 (11) ダウンロードアドレスは「○日まで利用可能」などの期限設定を可能とする機能を有すること。 (12) 添付ファイル付きメールを誤った送信先へ送付した場合、ダウンロードアドレスを使用停止できる機能を有すること。 (13) 添付ファイル付きメールを相手に送信する際、添付ファイルのファイルサイズによってサーバ上へ保管せずにメールを直接送付する機能を有すること。 (14) 添付ファイル付きメールを相手に送信する際、送信メールのFrom/To/Ccに特定文言が含まれている場合、添付ファイルのサイズによってサーバ上へ保管せずにメールを直接送付する機能を有すること。 (15) 個人フォルダは、他システムと連携して自動作成及び削除ができること。 (16) グループに登録したフォルダ・ファイルは、登録した本人の他にグループの管理者等必要な権限を有する者も変更・削除ができること。 (17) ユーザは複数のグループに属することができること。 (18) 学外者等本学のアカウントを持たないユーザにファイルを受け渡したいとき、当該ファイルのURLを通知し、アクセスしてもらうことでファイルの受け渡しができること。また、受け渡し可能な有効期限、利用回数、パスワードの設定ができること。 (19) 学外者等本学のアカウントを持たないユーザからファイルを受け取りたいとき、当該ファイルのURLを通知し、アクセスしてアップロードしてもらうことでファイルの受け取りができること。また、受け取りの有効期限、パスワードを設定で

	きること。 (20) 学外者等本学のアカウントを持たないユーザからファイルを受け取る際に、URLにアクセス後メールアドレスを入力させ、入力したメールアドレスへワンタイムパスワードを発行し、メールアドレスでの認証ができる機能を有すること。 (21) 指定日時を設定した場合、指定した日時に自動的にファイルを削除できる機能を有すること。 (22) 管理者の管理画面はWebブラウザで操作ができること。 (23) 管理画面から本サーバに対するSSL証明書を設定できること。 (24) 管理画面からオンラインストレージサーバソフトウェアのバージョンアップができること。 (25) Active Directory/LDAPとユーザーアカウント情報を連携できる機能を有すること。 (26) CSVファイルにてユーザーアカウントの追加・更新および一覧の取得を行えること。 (27) データベースを別途インストールしなくても動作する製品であること。 他のファイルサーバ上に存在する各ユーザのホームフォルダや共有フォルダをブラウザ上から参照、操作可能な機能を有すること。
その他	(1) 2.システム全般に関わる基本要求に準拠すること。