令　和　2　年　2　月　28　日
日　本　学　術　会　議　事　務　局
管　理　課　用　度　・　管　理　係

調　達　公　告

件　　名	メールホスティングサービス
ボックス番号	①
数　　量	一式
作 業 内 容	別紙仕様書の通り
契 約 期 間	令和2年4月1日から令和2年9月30日
見積提出期限	令和2年3月13日(金)正午 (郵送の場合は3月12日(木)18:00)
見積書提出先及び仕様書交付先	〒106-8555 東京都港区六本木7-22-34 内閣府日本学術会議事務局管理課用度・管理係 ℡03-3403-1930
担 当 者 名	用度・管理係　星・髙畑
仕様書問合せ先	内閣府日本学術会議事務局企画課情報係
担 当 者 名	情報係長　森田
競争に参加する者に必要な資格及び注意事項	○参加資格：令和01・02・03年度（平成31・32・33年度）全省庁統一参加資格 「役務の提供等」A、BまたはC等級に格付けされている者。 ○参加者は、見積書の提出をもって 「暴力団排除に関する誓約事項」（別記）に誓約したものとする。 ○その他：別添の「オープンカウンター方式について」を参照

別紙

仕　様　書

1　件　名

メールホスティングサービスの調達

2　履行期間

令和2年4月1日（水）～令和2年9月30日（水）

3　仕　様

インターネットを介したメール送受信を可能とするメールサーバ機能を提供すること。その際、次の（1）～（4）の条件を満たす（ア）～（ケ）のサービスを提供すること。

（1）日本学術会議のドメイン名の確保

①　『scj.go.jp』ドメインにてメールの送受信が行えること。

②　当該ドメイン名にて、日本学術会議ホームページと連携できること。

（2）ウイルスチェック

①　送受信時ともにコンピュータウイルスのチェックを行うこと。

②　24時間365日の運用体制でウイルスのパターンファイルの更新を行うこと。

③　24時間365日の運用体制でウイルスの検索エンジンの更新を行うこと。

（3）メールボックス

①　容量300GBのメールボックスを提供すること。

②　グループ設定が可能なこと。また、グループアドレスで受信したメールについて、各個人への自動転送設定が可能なこと。

③　アカウントの追加・削除、転送設定等がWebブラウザから可能なこと。

（4）情報セキュリティ対策

本業務を実施するに当たっては、「政府機関等の情報セキュリティ対策のための統一基準群」（平成30年7月25日サイバーセキュリティ戦略本部決定）、「政府機関等の対策基準策定のためのガイドライン」（平成30年7月25日内閣官房内閣サイバーセキュリティセンター）及び「内閣府本府情報セキュリティポリシー」等を遵守するものとする。また、情報セキュリティ対策に関する規定等が新たに策定又は改定された場合は、当該規定等に基づくこと。

加えて、これに関連して以下について対応すること。

・ 請負事業者は、本業務に関し内閣府の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順及び品質保証体制を証明する書類（例えば、品質保証体制の責任者及び各担当者がアクセス可能な範囲等を示した管理体制図）を契約日より 2 週間以内に提出すること。また、第三者機関による品質保証体制を証明する書類等が提出可能な場合は、合わせて提出すること。

・ 本調達に応札する者は、本業務を実施する請負事業の実施場所、請負事業従事者の所属（契約社員、派遣社員等の雇用形態は問わず、請負事業に従事する全ての要員）・専門性（情報セキュリティに係る資格・研修実績等）・実績（経験年数、資格等）及び国籍、請負者の資本関係・役員に関する情報に関する資料（書面の様式は問わない。ただし、別紙 2 と同様、住所、会社名及び同印、代表者名及び同印、連絡先（所属、担当者、電話番号）については記載すること。）を令和 2 年 3 月 6 日（金）正午までに提出すること。（なお、当該資料の提出については、情報セキュリティの確保を目的とするものであり、入札参加要件として用いることを目的とするものではない。）

・ 本業務に係る情報セキュリティ事故が発生した場合は、速やかに内閣府に報告し、了承を得た上で対策を実施すること。また、必要に応じて内閣府、又は内閣府が指定した者が実施する情報セキュリティ監査を受入れ、その指示に従うこと。

・ 本業務における情報セキュリティ対策の履行状況を確認するために、内閣府が情報セキュリティ対策の実績及び情報の秘密保持等に係る管理状況の報告を求めた場合、それに応じること。

（ア）メール基本機能

① アカウントは管理者と一般ユーザで区分でき、ともに複数作成できること。

② 管理画面として当局専用の Web インターフェースを提供し、メールアカウントの登録・変更・削除（個別の処理に加え、一覧を記載した csv 形式若しくはテキストファイルによる一括処理にも対応すること。）が可能であること。

③ 第三者によって不正アクセスや迷惑メール配信の中継地点として意図しない用途に使用されることを防ぐため、SMTP（Simple Mail Transfer Protocol）認証に対応する等必要な措置を講じること。

④ メール受信の際にパスワードを暗号化する POPS（Post Office Protocol over SSL）に対応すること。

⑤ メール送受信の際、TSL で暗号化した通信を行うこと。

⑥ メール送受信の通信経路上において、ユーザ ID、パスワード、メール本文を暗号化すること。

（イ）迷惑メール対策機能

① 迷惑メール判定エンジンはオープンソース製品を利用せず、仕様が一般に公開され

ていない商用ベンダーの製品を搭載していること。

② インターネットを経由して当局に届く電子メールについて、迷惑メール送信元・IP アドレスのリスト（ブラックリスト）を参照しつつ、サブジェクト・単語・内容などから総合的に迷惑メールかどうかを判定し、迷惑メールと思しきメールを隔離し（破棄はしないこと。）、正常なメールを配送すること。

③ ホワイトリスト機能として、予め登録したメールアカウント宛のみ配送するものとし、存在しないメールアカウント宛てのメール配送による永続エラーを防ぐこと。ホワイトリストはメールアカウントの登録から 30 分以内に反映されること。

④ 特定の送信元（メールアドレス、ドメイン及びサブドメイン）から送られたメールについて、メールアカウントごとに受信の許可・拒否を設定できること。

⑤ 迷惑メールと判定した場合、メールアカウントごとに最低でも以下の処理を選択できること。また、迷惑メールと思しきメールにはランク付け（点数・パーセンテージ化等）し、ランクに応じた制御が行えること。

－ 迷惑メールを隔離する。

－ 隔離等の処理を行わず、配送する。

⑥ 迷惑メールを隔離する保存領域をアカントごとに設け、一定期間（14 日間程度）保存できること。なお、迷惑メールに関する保存領域には容量制限を設けないこと。

⑦ 当局専用の管理画面として機能する Web インターフェースを提供し、システム管理者が全ユーザの隔離したメール情報の表示、迷惑メールの隔離設定（管理者側での一括若しくは個別設定）を行えること。

⑧ 各メールアカウント用の Web インターフェースも提供し、各ユーザ自身が隔離メールの管理（確認・リリース・設定変更）を可能とすること。

⑨ 上記⑧の Web インターフェースへは TLS（Transport Layer Security）によって暗号化された通信でアクセスできること。

⑩ 隔離された迷惑メールがある場合、各メールアカウントに対し「隔離通知メール」を送付する機能を有すること。形式はテキスト形式若しくは HTML 形式とする。

⑪ 「隔離通知メール」の送付間隔は、最低でも以下より選択できることとし、メールアカウントごとに任意の設定を行えること。ただし、その設定可否を制限できること。

－ 曜日又は日数での範囲指定

－ 送信しない

⑫ Web インターフェースはメールに含まれるスクリプト等が実行されない安全な環境であること。

⑬ 各ユーザ自身が「隔離通知メール」に表示された Web インターフェースへの URL から、Web インターフェースへログインし隔離されたメールをリリースできること。リリースした履歴は、管理者が Web インターフェースから確認できること。

⑭ メールに添付されるファイルの拡張子、ファイルタイプを判別して、受信拒否又は

隔離措置を取る設定が行えること。

（ウ）ウイルスメール対策機能

① インターネットから当局宛て、及び、当局からインターネット向けのメールを対象としたウイルスチェックを行い、メールに含まれるウイルスを検知・駆除すること。

② ウイルスを駆除した場合、駆除したことを受信者に通知できること。

③ 最新のウイルスに対応できるように、ウイルスのパターンファイルを常時最新の状態に保つこと。

④ 当局専用の管理画面として機能する Web インターフェースを提供し、システム管理者がウイルス定義ファイルの更新状況やウイルス駆除状況等を確認できること。

（エ）添付ファイル自動暗号化機能

① 送信メールの添付ファイルを自動的に暗号化する機能を有すること。

② 本機能の対象をメールアドレスやドメインの単位で有効化・無効化を個別設定できること。

③ 添付ファイルはパスワード付き zip ファイルに変換すること。パスワードはシステムが生成するランダムな文字列を自動で設定し、「パスワード通知メール」を送付できること。

④ 「パスワード通知メール」はシステムから自動送信され、その宛先を送信元若しくは送信先から管理者が一括で設定できること。

⑤ パスワード通知メールの件名と本文の文面を管理者設定より変更できること。

⑥ パスワードの文字数制限は 12 文字以上で設定できること。

⑦ 送信元において、メールごとに自動暗号化機能を回避する方法を有していること。（件名に特定の文言・文字列を含めることで回避できるなど。）

（オ）経路暗号化機能

① メールを送信する際、送信先が TLS に対応している場合は、経路を暗号化して通信を行うこと。なお、受信時においても送信元が TLS にて接続要求を行った場合は、TLS にて通信を行うこと。

② 送信元において特別な設定をすることなく暗号化を行うこと。

（カ）メールボックス機能

① メールボックスの利用率が一定の容量を超過した際は、警告メールを送付できること。

（キ）ログ管理／ダウンロード機能

① 障害時の原因解析などに利用するため､電子メールの送受信ログを 1 日単位で TSV（タブ区切り）形式若しくは CSV 形式により取得できること。

② ログの保存期間は 90 日間以上とする。

③ 送受信ログを解析した上で、グラフ等を用いて、メール流量、送受信者リスト（通数順)、ウイルス検出情報などの情報を表示できること。解析可能な期間は 90 日以上とする。

（ク）誤送信防止機能

① 誤送信防止のため、一時的にメールの配送を保留する機能を有すること。

② 配送保留された送信メールの保留時間は、5 分～60 分以上の間で、1 分単位で設定できること。

③ 送信メールが配送保留され一定時間経過した場合は、保留されている送信メールの操作について、自動送信・自動削除から選択可能であること。

④ 送信メールが配送保留された場合、送信元宛てに「保留通知メール」を送付できること。また、送信元が配送保留された送信メールの送信・削除の操作ができること。

⑤ 本機能の対象をメールアドレスやドメインの単位で有効化・無効化を個別設定できること。

（ケ）なりすましメール対策機能

① なりすましメールを防ぐための送信ドメイン認証として SPF（Sender Policy Framework：RFC4408）及び DKIM（DomainKeys Identified Mail：RFC4871）に送受信とも対応していること。また、受信するメールに対して SPF と DKIM の認証処理を行い、メールヘッダ等に検証結果を付記できること。

② 当局より送信されるメールが他組織にて受信される際にも送信ドメイン認証が適切に行われるよう、メールヘッダへの DKIM 署名の付与が可能であること。

③ SPF を検証し、送信元が SPF に対応していない場合に、SPF 非対応の旨を示す文字列をサブジェクトに挿入できること。また、任意のドメインに対して、SPF に対応していない場合に、メールの受信を拒否する設定が可能であること。

④ 受信するメールに対して、DMARC（Domain-based Message Authentication, Reporting and Conformance） の認証結果をメールヘッダに付与し、認証結果に基づいて受信拒否や隔離といった処理が可能であること。

⑤ 当局のドメインを詐称したメールを用いて第三者のメールサーバで意図的なエラーを発生させ、大量のバウンスメール（エラーメール）として当局のメールサーバに送られてくることを防ぐ機能を備えること。

４　サポート窓口

電話、電子メール等による対応サポート窓口を提供すること。

５　その他　（事業者要件）

本業務は、複雑かつ高難度の作業を長期間継続的に実施する必要があり、請負事業者には高い専門性と豊富な経験及び実績が求められる。本調達における事業者要件は以下のとおり。

（１）令和 01・02・03 年度（平成 31・32・33 年度）内閣府競争参加資格（全省庁統一資格）「役務の提供等」の「A」、「B」又は「C」の等級に格付けされている者であること。

（２）1,000 アカウント以上のメールホスティングサービスの提供実績が過去 3 年以内に 3 件以上あること。

（３）プロジェクトマネジメントに関する公的資格（情報処理技術者試験プロジェクトマネージャー、PMP 等相当資格）を有し、本業務と同程度の開発をプロジェクトマネージャーとしてリードした経験が 10 年以上ある要員を含めること。

（４）本サービス提供者には、ITIL（エキスパート、マスター）または情報処理技術者試験 IT サービスマネージャ認定資格を持つ要員を含めること。

（５）ISO9001 又は CMMI レベル 3 以上の認証のいずれかの取得、もしくは同等の品質マネジメントシステムを確立していること。

（６）ISO.IEC27001 又は JIS Q27001 認証のいずれかの取得、もしくは同等の情報セキュリティマネジメントシステムを確立していること。

（７）環境マネジメントシステム規格である ISO14001 の認証を受けていること、又はエコ・ファースト企業として認定されていること。

（８）政府若しくは自治体関連へのシステム開発及び情報処理業務等を過去 3 年以内に複数件行った実績があること。

別　記

暴力団排除に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記事項について入札書又は見積書の提出をもって誓約します。

この誓約が虚偽であり、又はこの誓約に反したことにより、当方が不利益を被ることとなっても、異議は一切申し立てません。

また、貴職の求めに応じて当方の役員名簿（有価証券報告書に記載のもの（生年月日を含む。）ただし、有価証券報告書を作成していない場合は、役職名、氏名、性別及び生年月日の一覧表）等を提出すること、及び当該名簿に含まれる個人情報を警察に提供することについて同意します。

記

1　次のいずれにも該当しません。また、当該契約満了まで該当することはありません。

(1)　契約の相手方として不適当な者

ア　法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。以下同じ。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）第２条第２号に規定する暴力団をいう。以下同じ。）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき

イ　役員等が、自己、自社若しくは第三者の不正の利益を図る目的、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

ウ　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

エ　役員等が、暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき

オ　役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

(2)　契約の相手方として不適当な行為をする者

ア　暴力的な要求行為を行う者

イ　法的な責任を超えた不当な要求行為を行う者

ウ　取引に関して脅迫的な言動をし、又は暴力を用いる行為を行う者

エ　偽計又は威力を用いて契約担当官等の業務を妨害する行為を行う者

オ　その他前各号に準ずる行為を行う者

2　暴力団関係業者を下請負又は再委託の相手方としません。

3　下請負人等（下請負人（一次下請以降の全ての下請負人を含む。）及び再受託者（再委託以降の全ての受託者を含む。）並びに自己、下請負人又は再受託者が当該契約に関して個別に締結する場合の当該契約の相手方をいう。）が暴力団関係業者であることが判明したときは、当該契約を解除するため必要な措置を講じます。

4　暴力団員等による不当介入を受けた場合、又は下請負人等が暴力団員等による不当介入を受けたことを知った場合は、警察への通報及び捜査上必要な協力を行うとともに、発注元の契約担当官等へ報告を行います。