

2026 年 10 月 8 日

2026 年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」に 関する入札のご案内

一般社団法人 JPCERT コーディネーションセンター
(入札管理責任者 総務部長 高崎 三千雄)

次のとおり一般競争入札に付します。

1. 入札に付する事項

- (1) 名 称: 2026 年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」
- (2) 内 容 等: 別紙 1 のとおり
(2026 年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」仕様書)
- (3) 履 行 期 限: 別紙 1 のとおり
(2026 年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」仕様書)

(4) 入札方法等:

本件は、JPCERT コーディネーションセンター（以下「JPCERT/CC」）が経済産業省から委託されている令和 8 年度サイバーセキュリティ経済基盤構築事業(サイバー攻撃等国際連携対応調整事業)で実施されるプロジェクトの一つとして実施し、入札は総合評価落札方式で行う。

したがって、入札の際には提案書を提出し、技術審査を受けなければならない。

本入札の履行によって新たに作成された成果物に係る著作権その他の知的財産権は、JPCERT/CC に譲渡されるものとし、その対価は入札額に含まれるものとする。

入札者は消費税および地方消費税に係る課税事業者であるか免税事業者であるかに関わらず、入札書には税抜きの金額を記載すること。

2. 入札要件

予算決算および会計令（以下「予決令」）第 70 条の規定に該当しない者であること。ただし、未成年者、被保佐人または被補助人であって、契約締結のために必要な同意を得ている者は、参加することを認める。

- (1) 予決令第 71 条の規定に該当しない者であること。
- (2) 経済産業省から補助金交付等停止措置または指名停止措置が講じられている者ではないこと。
- (3) 経営の状況、信用度が極度に悪化していないと認められる者であり、適正な契約の履行が確保される者であること。
- (4) 入札案件に対し、原則として再委託を行わないこと。ただし、事業全体の企画および立案ならびに根幹に関わる執行管理以外の業務を再委託する場合であって、再委託額が入札額の 50%未満であ

り、かつ 100 万円（消費税込）以下の軽微な再委託に該当するか、または経済産業省からの承認がある時は再委託を認める。

(5) 入札説明会に参加し、入札説明書の交付を受けた者であること。

(6) その他必要な事項については、JPCERT/CC が入札説明会で配布する資料に従うこと。

3. 入札者の提出書類

入札参加希望者は、JPCERT/CC が配布する仕様書に基づいて提案書を作成し、受領期限内に提出しなければならない。また、落札者の決定日前日までの間において JPCERT/CC から当該書類に関して説明を求められた場合は、これに応じなければならない。なお、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

4. 契約事項を示す場所等

(1) 入札説明会の日時および場所

日時：2026 年 10 月 28 日（水）16:00～17:00（1 時間程度を予定）

場所：東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階

JPCERT コーディネーションセンター

TEL：03-6271-8901

FAX：03-6271-8908

※ 説明会参加希望者は、10 月 22 日（木）17:00 までに必要事項（法人名、部署名、参加者氏名、連絡先）を記載の上、メールにて参加を申し込むこと（送付先：dc-info@jpcert.or.jp）

(2) 提案書等の受領期限および受領場所

期限：2026 年 11 月 12 日（木）17:00（必着）

場所：「4. 契約事項を示す場所等」(1) に同じ

方法：持参、郵便（簡易書留による）

(3) 入札者決定の通知日

2026 年 11 月 16 日（月）

(4) 入札日

日時：2026 年 11 月 18 日（水）16:00～（落札者が決定するまで）

場所：「4. 契約事項を示す場所等」(1) に同じ

5. その他

(1) 入札保証金および契約保証金

全額免除

(2) 入札書の変更および取り消し

入札者は、提出した入札書等の変更および取り消しをすることができない。

(3) 入札の無効

本公告の 2. 入札要件に示す入札参加資格のない者による入札および各項に定めた諸条件について、その条件に違反した場合は入札を無効とする。

(4) 契約書の作成

落札者が JPCERT/CC と契約を締結する際には、契約書の作成を必要とする。

(5) 支払条件

検収合格後、JPCERT/CC が実施する確定検査（支出計画書とおりに経費が適正に支出されたかの確認）後に契約額が確定する。なお、契約額の上限は落札額とする。

(6) 落札者の決定方法

予決令第 79 条の規定を参考に作成された予定価格の制限の範囲内で、入札管理責任者が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、入札管理責任者が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされない恐れがあると認められるとき、またはその者と契約することが公正な取引引きの秩序を乱すこととなる恐れがあつて著しく不適當であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者としてすることがある。なお、再委託がある場合は、別途、経済産業省からの承認が必要である。

6. 問い合わせ先（メールでの問い合わせを原則とする）

(1) 入札説明書等に関する問い合わせ

JPCERT/CC

国内コーディネーショングループ 椎木（しいぎ）／吉岡（よしおか）

Email : dc-info@jpcert.or.jp

(2) 入札行為に関する問い合わせ

JPCERT/CC

総務部 鈴木（すずき）／神山（かみやま）

Email : soumu@jpcert.or.jp

※緊急を要する場合に限り、電話による問い合わせが可能

月～金曜日（祝・休日を除く）、9:00～18:00（12:00～13:00は除く）

TEL : 03-6271-8901（※留守番電話対応中のため、用件を録音してください）

2026年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」仕様書

1. 件名

2026年度「フィッシング対策協議会 報告受け付け用メールサーバー構築」

2. 目的

JPCERTコーディネーションセンター（以下「JPCERT/CC」）は、フィッシング対策協議会が実施するフィッシング報告受け付けの活動を支援している。本業務は、外部からの報告を受け付ける現行メールサーバーの更新に伴い、国内VPS上に、オープンソースソフトウェアを用いたメールサーバーを設計、構築および移行し、安定的かつ安全に運用できる環境を整備することを目的とする。

新環境では、最大1日約54,000件の受信メールを安定して処理するとともに、送信ドメイン認証、メーリングリスト、サーバー側メール振り分け、マルウェア検査・隔離、監視およびバックアップ等の機能を提供する。

3. 事業の内容および実施方法

(1) 業務範囲

- ① 要件確認ならびに基本設計および詳細設計
- ② 国内VPSの選定支援、必要スペックおよび容量の算定
- ③ OS、メール関連ソフトウェアおよび監視・セキュリティ関連ソフトウェアの導入・設定
- ④ DNS、送信ドメイン認証およびTLSに関する設定支援
- ⑤ 現行環境からのアカウント、メーリングリスト、エイリアス、転送設定その他設定情報の移行
- ⑥ 試験、移行、並行稼働、切り替えおよび切り戻し計画の作成・実施
- ⑦ 運用手順書等の成果物作成および管理者向け説明
- ⑧ 構築完了時の引き継ぎ

(2) 構築基本方針

- ① JPCERT/CCがVPSの契約主体となり、VPSおよびシステムの管理権限を保持すること。
- ② セキュリティ上の影響範囲を分離するため、外部とのメール送受信を行うMX・メーリングリストサーバーと、メールを保存し利用者へ提供するIMAPサーバーは、別々のVPSとして構築すること。
- ③ 特定事業者の独自技術に過度に依存せず、後継事業者が運用を引き継げる構成とすること。
- ④ 「（4）現行環境および利用規模」を最低限満たす範囲で、具体的な構成、容量および管理

方式は受注者が提案すること。

- ⑤ 不正メールの報告受け付けを主要用途とするため、調査対象メールを一律に拒否または削除しないこと。

(3) 履行期間およびスケジュール

項目	要件
構築・移行期間	契約締結日から 2027 年 2 月 26 日まで。本稼働は同日までに開始すること。
運用保守期間	見積もりを提案すること。次年度以降に別途契約し定める。
並行稼働	現行環境との並行稼働を可能とし、期間は移行計画において JPCERT/CC と協議して定める。
停止時間	MX 切り替え等に伴う停止時間は JPCERT/CC と調整する。受注者は停止時間を最小化する計画を提示すること。

受注者は、契約後速やかに、設計、構築、試験、移行リハーサル、並行稼働、本番切り替えおよび検収を含む工程表を提出し、JPCERT/CCの承認を得ること。

(4) 現行環境および利用規模

項目	要件
現行設置形態	クラウドサーバー
現行ソフトウェア	SMTP：Postfix、POP/IMAP：Dovecot、メーリングリスト：fml
受信メール数	約 13,500～54,000 件／日
メールアカウント数	20～30 アカウント
利用者数	約 10 名
管理者数	2 名
IMAP4 サーバー	ディスク容量 120GB（メールストア領域 80GB、システム領域 40GB） 直近 2 日間分のメールデータのバックアップを保持している。
MX・ML サーバー	ディスク容量 60GB（システム・メーリングリストデータ領域 40GB、 バックアップ・作業領域 20GB）MX サーバーがメーリングリスト機能

項目	要件
	を兼ねる。
現行総容量	2 台合計 180GB。上記は現行環境の割り当て容量であり、新環境に必要な容量を指定するものではない。
メーリングリスト	約 20 リスト。メンバー数は平均約 60 名、最大約 370 名であり、今後増加する可能性がある。
既存ドメイン	既存の独自ドメインを継続利用する。サブドメインを利用できる。
DNS 管理	JPCERT/CC による管理を想定する。

(5) 基盤およびソフトウェア要件

① 国内VPS

- (ア) 日本国内のデータセンターで稼働するサービスであること。
- (イ) 固定グローバルIPv4 アドレスを利用できること。
- (ウ) SMTP通信に必要なポートを利用でき、メールサーバー用途が利用規約上認められていること。
- (エ) 逆引きDNS (PTRレコード) を設定できること。
- (オ) ディスク容量を拡張できること。
- (カ) スナップショットまたはバックアップを取得できること。
- (キ) VPSの契約および管理権限をJPCERT/CCが保持できること。
- (ク) MX・メーリングリストサーバーとIMAPサーバーを別々のVPSとして構築できると。
- (ケ) 両サーバー間の通信は、送信元、送信先、ポートおよび通信方向を必要最小限に制限すること。MX・メーリングリストサーバーからIMAPサーバーへのメール配送、その他必要な通信のみを許可すること。

受注者は、本仕様書に示す処理量、保存期間、ログ、隔離領域、メーリングリストアーカイブおよびバックアップを考慮し、必要なCPU、メモリ、ディスクおよびネットワーク性能を算定して提案すること。

IMAPサーバーのメモリは32GB以上とすること。受注者がメール振り分け、インデックス作成、同時接続数その他の処理を踏まえて、これを超える容量が必要と判断する場合は、算定根拠とともに提案すること。MX・メーリングリストサーバーのメモリその他のスペックは受注者が算定して提案すること。

② OS

OSは、Ubuntu ServerまたはRocky Linuxの安定版を使用すること。構築時点において、原

則として3年以上のセキュリティアップデート提供期間が残っているバージョンを採用し、採用するOSおよびバージョンはJPCERT/CCと協議のうえ決定すること。

③ 基本ソフトウェア

項目	要件
SMTP	Postfix を基本とする。
POP/IMAP	Dovecot を基本とし、IMAP に対応すること。POP には対応しない。
メーリングリスト	Mailman を基本とする。採用するメジャーバージョンとサポート方針を提案すること。
振り分け	Dovecot Sieve 等によるサーバー側振り分けを提供すること。
Web メール	必須としない。必要性および導入効果がある場合は提案事項とする。
独自管理機能	必須としない。OSS の管理機能を補完する統合管理画面等は提案事項とする。

(6) 機能要件

① メール送受信

- (ア) 独自ドメインによるメール送受信に対応すること。
- (イ) 利用者はIMAPSを用いてメールを利用し、メールの正本をIMAPサーバー上に保持すること。
- (ウ) 外部とのメール送受信および利用者からのメール送信受け付けは、MX・メーリングリストサーバーで行うこと。
- (エ) SMTP AUTHのアカウントおよび認証機能はMX・メーリングリストサーバーのみに設定し、IMAPサーバーには外部向けのSMTP AUTH機能を設けないこと。
- (オ) 通常メールおよびメーリングリストによる配信を安定して処理できること。
- (カ) 1通当たり50MB以上のメールを取り扱えることとし、実際の上限値はJPCERT/CCと協議して設定すること。
- (キ) 配送に失敗または遅延したメールについて、管理者が配送状況および原因を確認できること。
- (ク) 一時的な配送失敗は自動的に再送し、恒久的な配送失敗は送信者または管理者が確認できること。

② 処理性能

- (ア) IMAPサーバーにおいて少なくとも約54,000件／日のメールを受信・保存できる処理

能力を有すること。

- (イ) MX・メーリングリストサーバーは、少なくとも約54,000件／日の外部メールを受信し、IMAPサーバーへの中継処理を安定して行えること。また、外部受信および内部中継を合わせ、1日当たりおおむね100,000件以上の配送処理を安定して行えること。
- (ウ) 送信件数は業務状況によって変動するため固定値を設定しない。ただし、1メーリングリスト当たり最大370名に対する配信を遅滞なく処理できること。
- (エ) 受注者は、メールの到着が短時間に集中することを考慮し、想定するピーク時の受信件数、同時SMTP接続数、キュー滞留量および処理時間を提示すること。試験条件はJPCERT/CCと協議して決定すること。

③ 通信の暗号化およびメール送信

- (ア) 利用者端末からMX・メーリングリストサーバーへのメール送信には、サブミッションポートを使用し、STARTTLSまたは接続開始時からTLSにより暗号化する方式を使用すること。TLS接続が確立する前のSMTP AUTHおよび暗号化されていない通信による認証を許可しないこと。
- (イ) MX・メーリングリストサーバーは、外部メールサーバーとの送受信においてSTARTTLSに対応すること。外部への配送時は、配送先がSTARTTLSに対応している場合にTLSを使用すること。
- (ウ) 外部からの受信について、TLSを使用しないメールを拒否するか否かは、フィッシング報告の到達性を考慮してJPCERT/CCと協議のうえ設定すること。
- (エ) MX・メーリングリストサーバーとIMAPサーバーとの通信は、プライベートネットワーク等の外部から直接接続できない経路を使用すること。これを利用できない場合は、TLSによる暗号化および接続元IPアドレス制限を実施すること。

④ メーリングリスト

- (ア) 約20リストを運用でき、リストおよびメンバー数を拡張できること。
- (イ) リストごとに管理者、投稿者、参加者、配信条件等を設定できること。
- (ウ) メンバーの追加・削除その他の管理を、権限を付与された管理者が実施できること。
- (エ) 配信メールのアーカイブ機能を有し、その閲覧を管理者に限定できること。
- (オ) アーカイブはバックアップ対象とし、必要時に復元できること。

⑤ サーバー側メール振り分け

- (ア) メールクライアントを常時起動することなく、サーバー上で受信メールを自動的に振り分けられること。
- (イ) 差出人、宛先、件名、本文およびその他のメールヘッダーを条件として利用できること。
- (ウ) 指定フォルダーへの移動、転送その他の合理的な処理を設定できること。
- (エ) 利用者または管理者が、振り分け条件を登録、変更および削除できる管理手段を提供すること。

- (オ) 文字コード、HTMLメール等により本文条件が適用できない場合の制約を明示すること。

⑥ DNSおよび送信ドメイン認証

- (ア) 既存ドメインおよび必要に応じたサブドメインを利用すること。
- (イ) MX、A/AAAA（利用する場合）、PTR、SPF、DKIMおよびDMARCレコードの設計・設定を支援すること。
- (ウ) 送信メールへのDKIM署名および受信メールのSPF、DKIM、DMARC検証に対応すること。
- (エ) DMARCポリシーおよびレポート受信先は、JPCERT/CCと協議して設定すること。

(7) セキュリティ要件

① アクセス管理

- (ア) 管理者アクセスにはIPアドレス制限および多要素認証を適用すること。ただし、OSへのアクセス等で多要素認証の直接適用が困難な場合は、VPN、踏み台サーバー、公開鍵認証等を組み合わせた代替策を提案すること。
- (イ) 管理者2名に対して個別の管理者アカウントを付与し、共有アカウントの常用を避けること。
- (ウ) 管理権限を必要最小限とし、管理操作を記録すること。
- (エ) 不要なサービスおよびポートを停止し、不正中継を防止すること。
- (オ) IMAPサーバーはインターネットからの不特定の接続を受け付けない構成とし、IMAPSによる利用者接続はJPCERT/CCが指定する接続方法に限定すること。その他の接続元からのIMAPおよびIMAPS通信をファイアウォール等により遮断すること。
- (カ) 接続元として許可する固定IPアドレスは、運用開始後に追加、変更および削除できること。設定変更の手順を運用手順書に記載すること。
- (キ) IMAPサーバーは、MX・メーリングリストサーバーからのメール配送に必要な通信のみを受け付け、接続元IPアドレス、宛先ポートおよび通信方向を必要最小限に制限すること。

② 不正メール・マルウェア対策

- (ア) 不正メールの報告受け付けを主要用途とするため、スパム判定による一律の受信拒否または自動削除を原則として行わないこと。
- (イ) スパム判定機能を用いる場合は、判定結果をヘッダー等に付与する方式を基本とし、挙動をJPCERT/CCと協議すること。
- (ウ) マルウェアまたは不正な添付ファイルを検知したメールは、通常のメールボックスから分離した領域へ隔離すること。
- (エ) 隔離メールは、権限を付与された管理者のみが確認、取得、復元または削除できること。
- (オ) 隔離時に管理者へ通知し、原則としてメール原本および添付ファイルを改変せず保持

すること。

- (カ) 隔離メールの保存期間は1カ月を初期値とし、JPCERT/CCと協議して変更できること。

③ 脆弱性およびパッチ管理

- (ア) OSおよび各ソフトウェアのセキュリティ情報を継続的に確認すること。
- (イ) セキュリティパッチは、影響を確認した上で合理的な期間内に適用すること。重大な脆弱性については、緊急性を踏まえJPCERT/CCと協議して速やかに対応すること。
- (ウ) 適用にサービス停止を伴う場合は、原則として事前にJPCERT/CCと調整すること。ただし、緊急対応では事後報告を認める。

④ TLSサーバー証明書

- (ア) 公的に信頼された認証局が発行するTLSサーバー証明書を使用すること。
- (イ) ACME等の標準的な仕組みを利用し、証明書の取得、更新、所定位置への配置、権限設定およびPostfix、Dovecotその他証明書を使用するサービスへの適用までを自動的に実行できること。
- (ウ) 証明書の有効期間が将来短縮された場合でも、手動更新を常態化させることなく、安全に更新できる構成とすること。
- (エ) 自動更新後に、新しい証明書が各サービスへ正しく適用され、TLS接続で提示されていることを確認できること。
- (オ) 自動更新、サービスへの適用または適用確認に失敗した場合は、速やかに管理者へメールで通知すること。
- (カ) 証明書の有効期限を監視し、残存期間が設定したしきい値を下回った場合は管理者へ通知すること。しきい値は証明書の有効期間に応じて変更できること。
- (キ) 秘密鍵を適切なアクセス権限で保護し、更新前後の証明書および秘密鍵を安全に管理すること。

(8) 不正接続およびリソース枯渇対策

- ① 攻撃または異常な通信によって、CPU、メモリ、ディスク、プロセス、ファイルディスクリプター、メールキューその他のリソースが枯渇し、通常業務に支障が生じることのないよう設計すること。
- ② IMAPサーバーは、利用者数、利用端末数およびメールクライアントが生成する複数接続を考慮し、通常業務に支障を生じさせず、かつ不正接続によるリソース枯渇を防止できるよう同時接続数、利用者ごとの接続数、タイムアウトおよびプロセス数を設定すること。
- ③ 異常な接続、認証失敗、送信量、キュー滞留およびリソース使用量を監視し、設定したしきい値を超えた場合は管理者へ通知すること。

(9) 容量、保存、バックアップおよびログ

- ① 容量設計

現行環境の総ディスク容量180GBおよび受信メール数の約54,000件／日を参考として、メールアドレス、メーリングリストデータ、ログ、隔離メール、作業領域、インデックス、オフライン保管およびバックアップに必要な容量を算定し、適切なサーバー構成および初期ディスク容量を根拠とともに提案すること。現行の180GBは割り当て容量であり、新環境の最低容量または指定容量を意味しない。総メモリ容量も受信メール数やサーバー側でのメール振り分け処理、マルウェア処理を適切に実行するために必要な容量を算定し提案すること。

容量の算定に当たっては、OSおよび導入ソフトウェア、メールストア、メーリングリストデータ、ログ、隔離領域、インデックス、作業領域、バックアップその他運用に必要な領域を区分して示すこと。また、運用保守期間中のデータ増加および一定の空き容量を考慮すること。

ディスク、メモリ使用率を監視し、容量不足が予見される場合はJPCERT/CCへ通知すること。サービス停止を伴わず、または停止を最小限として容量を拡張できる構成とし、容量追加時の作業内容、サービスへの影響およびVPS利用料その他の費用を示すこと。

② バックアップ

- (ア) メールデータ、設定情報、アカウント情報、メーリングリスト情報および必要なアーカイブをバックアップ対象とすること。
- (イ) バックアップは1日1回以上取得し、1カ月間保存すること。具体的な世代管理方式は受注者が提案すること。
- (ウ) 構築時に復元試験を実施し、メールデータおよび設定情報を復元できることを確認すること。
- (エ) バックアップ先、暗号化、アクセス権限およびVPS障害時の利用可否を明示すること。

③ オフライン保管

容量管理のため、指定期間のメールを1カ月単位等で外部媒体または外部ストレージへ出力し、出力結果を確認した後にサーバーから削除できる機能または手順を提供すること。常時検索・閲覧する機能は不要とし、必要時にサーバーへ復元できること。保存形式および復元手順は、特定製品に過度に依存しないものとする。

④ ログ

- (ア) メール送受信、配送、認証、管理操作、マルウェア検知、隔離およびシステム動作に関するログを取得すること。
- (イ) ログは原則として15カ月分を保存すること。必要容量および保存方式を提案すること。
- (ウ) ログへのアクセスを管理者に限定し、改ざんおよび不正削除を防止すること。
- (エ) 障害、不達およびセキュリティ事象の調査に必要な検索・抽出手段を提供すること。

(10) 移行要件

① 移行対象

項目	要件
メールデータ	過去メールの一括移行は行わない。現行サーバー上のメールデータの扱いは切り替え計画で定める。
アカウント	メールアカウント、認証・権限情報および必要なメールボックス設定を移行する。
メーリングリスト	fml から Mailman へ、リスト名、メンバー、管理者、投稿権限、配信条件その他必要な設定を移行する。
その他設定	エイリアス、転送設定、振り分けルールその他 JPCERT/CC が指定する設定を、技術的に可能な範囲で移行する。

② 移行計画

- (ア) 現行環境の設定およびデータを事前に調査し、移行可否、移行方法および制約を明示すること。
- (イ) 移行リハーサルを行い、件数、設定値および動作を照合すること。
- (ウ) 並行稼働、DNS変更、利用者周知、本番切り替え、確認および切り戻しを含む計画を提出すること。
- (エ) 切り替え後、メール送受信、認証、振り分け、ML配信および送信ドメイン認証を確認すること。

(11) 監視および運用保守

監視および運用保守は構築とは別契約を想定しているため、下記要件を対応した費用を提案すること。

① 監視

- (ア) 24時間365日の死活監視を実施すること。
- (イ) 死活監視に加え、CPU、メモリ、ディスク使用率、メールキュー、主要プロセス、証明書有効期限等について、必要性和費用を含めて提案すること。
- (ウ) 障害またはしきい値超過を検知した場合、指定されたJPCERT/CCのメールアドレスへ通知すること。
- (エ) 監視通知先自体が利用不能となる事態を考慮し、外部メールアドレス等を通知先として設定できること。

② 障害対応

項目	要件
受け付け・検知	24 時間 365 日

項目	要件
一次通知	重大障害を検知後、原則として 30 分以内
対応開始	重大障害を検知後、原則として 1 時間以内。24 時間対応と平日対応の 2 種類を提案すること。
復旧目標	重大障害は 4 時間以内を目標とする。ただし、冗長化を行わないため、VPS 基盤障害、広域障害その他受注者が管理できない事象は除き、経過報告および代替・復旧策を提示すること。
障害報告	重大障害について、復旧後 5 営業日以内を目安に原因、影響、対応および再発防止策を報告すること。

③ 保守範囲

- (ア) 障害の切り分け、復旧、原因調査および再発防止対応
- (イ) OSおよび導入ソフトウェアのセキュリティアップデート
- (ウ) 証明書、DNS、メール配送、ブラックリスト登録等に関する技術的な調査・対応
- (エ) バックアップの取得および必要時の復元支援
- (オ) 設定変更のうち、障害対応または保守上必要なもの

(12) テスト

- ① メール送受信およびIMAPS接続試験
- ② STARTTLSおよび管理者アクセス制御の確認
- ③ SPF、DKIMおよびDMARCの送受信確認
- ④ メーリングリストの管理、投稿、最大370名を想定した配信およびアーカイブ確認
- ⑤ 差出人、件名、本文等を条件としたサーバー側振り分け試験
- ⑥ マルウェア検知、隔離、通知、管理者による確認および復元試験
- ⑦ TLSサーバー証明書の自動取得・更新・配置・サービス適用・適用確認および有効期限監視の試験ならびに更新失敗時の通知試験
- ⑧ バックアップおよび復元試験
- ⑨ 監視、障害通知、ログ記録およびログ検索試験
- ⑩ アカウント、MLおよびその他設定の移行結果確認
- ⑪ 必要に応じた性能・負荷試験

4. 必須要件

- ・ Linuxメールサーバーの構築経験を有すること
- ・ 本仕様書に定める構築、移行、試験、監視、障害対応および契約終了時の引き継ぎを履行できる体制を有すること
- ・ 類似規模または類似用途のメールサーバー構築・移行実績

5. 再委託

再委託がある場合は提案書に明記すること。ただし、事業全体の企画および立案ならびに根幹に関わる執行管理以外の業務を再委託する場合であって、再委託額が入札額の 50%未満であり、かつ 100 万円（消費税込）以下の軽微な再委託に該当するか、または経済産業省からの承認がある時は再委託を認める。

6. 履行期間

2027年2月26日（金）までに納品すること。検収期間については、納品後から2027年3月31（水）までとする。

7. 成果物

項目	要件
計画・管理	構築スケジュール、課題管理
設計	基本設計書、詳細設計書（基本と詳細を兼ねても可）、サーバー・ネットワーク構成図、パラメーターシート、ソフトウェア・バージョン一覧
移行	移行計画書、切り替え・切り戻し手順書、移行結果報告書
試験	試験計画書、試験項目書、試験結果報告書
運用	管理者向け操作手順書、監視・障害対応手順書、バックアップ・復元手順書、オフライン保管・復元手順書
完了	構築完了報告書、引き継ぎ資料

- ・ 上記の内容を格納した電子媒体（CD／DVD-R等）正副各1部

8. 納入場所

一般社団法人 JPCERT コーディネーションセンター

JPCERT/CCにおける入札は当該箇所につき以下の予算決算および会計令（国による歳入徴収、支出、支出負担行為、契約等について規定したもの）を準用して行うこととする。

予算決算及び会計令（抜粋）
（昭和22年4月30日勅令第165号）

（一般競争に参加させることができない者）

第70条 契約担当官等は、売買、貸借、請負その他の契約につき会計法第29条の3第1項の競争（以下「一般競争」という。）に付するときは、特別の理由がある場合を除くほか、当該契約を締結する能力を有しない者及び破産者で復権を得ない者を参加させることができない。

- 一 当該契約を締結する能力を有しない者
- 二 破産手続開始の決定を受けて復権を得ない者
- 三 暴力団員による不当な行為の防止等に関する法律（平成三年法律第七十七号）第三十二条第一項各号に掲げる者

（一般競争に参加させないことができる者）

第71条 契約担当官等は、次の各号の一に該当すると認められるときは、その者について三年以内の期間を定めて一般競争に参加させないことができる。その者を代理人、支配人その他の使用人として使用する者についても、また同様とする。

- 一 契約の履行に当たり故意に工事、製造その他の役務を粗雑に行い、または物件の品質若しくは数量に関して不正の行為をしたとき。
 - 二 公正な競争の執行を妨げたときまたは公正な価格を害し若しくは不正の利益を得るために連合したとき。
 - 三 落札者が契約を結ぶことまたは契約者が契約を履行することを妨げたとき。
 - 四 監督または検査の実施に当たり職員の職務の執行を妨げたとき。
 - 五 正当な理由がなくて契約を履行しなかつたとき。
 - 六 契約により、契約の後に代価の額を確定する場合において、当該代価の請求を故意に虚偽の事実に基づき過大な額で行つたとき。
 - 七 この項（この号を除く。）の規定により一般競争に参加できないこととされている者を契約の締結または契約の履行に当たり、代理人、支配人その他の使用人として使用したとき。
- 2 契約担当官等は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる。