

クラウド型不審メール対策サービスの利用契約

仕様書

日本原子力研究開発機構
システム計算科学センター
サイバーセキュリティ統括室

1. 概要

本仕様書は、クラウド型不審メール対策サービスの利用契約について、要件をまとめたものである。

2. 目的

日本原子力研究開発機構（以下、「機構」という）は、原子力に関する我が国唯一の総合的研究開発機関として、世界中の中核的拠点となることを目指している。その実現のため、機構の職員等は世界中の機構内外関係者と研究情報等の交換を行っており、その手段の1つとして世界中の関係者と手軽にかつ瞬時に文章や電子ファイル等を送受信可能な電子メールシステムを利活用している。

電子メールは、利便性が高く多くの利用者が情報交換の手段として用いる一方で、迷惑メールや組織内の情報窃取等を目的とした標的型攻撃メール等の不審メールが増加している。

不審メールは、日々手口が巧妙化及び多様化していることから、その対策には不審メールの検知率向上に向けた機能追加を含む新たな攻撃への迅速な対処及びそれらを実施しても滞りなく処理できるシステムが求められる。

そのため、機構ではクラウド型不審メール対策サービスを導入・運用しており、引き続き不審メール対策を継続する必要があることからクラウド型スパムメール対策サービスを利用する。

3. 仕様

3.1 に示す「品名及び数量」及び 3.2 に示す「要件」を満たすサービスを提供すること。

3.1 品名及び数量

本サービスは、SaaS (Software as a Service) 型クラウドサービスでの導入とする。

表 1：品名及び数量

No	品名	数量	備考
1	Fortimail Cloud Gateway Premium ※相当品を可とする。	1 式	アカウント数：8,200

3.2 要件

3.2.1 事業者に関する要件

- (1) 意図しない変更や機密情報の盗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や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や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。ISO9001 又は JIS_Q9001 の認証書類の提出でも可とする。
- (2) 情報セキュリティ管理体制が整っていることを証明する書類を提出すること。ISO/IEC27001、JIS_Q27001 認証又は ISMS 認証のいずれかの認証書類の提出でも可とする。

3.2.2 クラウドサービスに関する要件

- (1) 政府情報システムのためのセキュリティ評価制度(ISMAP)の ISMAP クラウドサービスリストにサービスが登録されていること。

3.2.3 不審メール対策サービスに関する要件

- (1) 機構が保持する 8,200 アカウントのメールアドレスによる受信処理に耐えうること。
なお、複数のドメインに対応可能でドメインごとのポリシーを定義可能であること。
- (2) サービス品質目標として、サービスの可用性及びメールの処理にかかる時間の目標値を定め、1 か月の稼働率が 99.99%以上の可用性を持つこと。なお、毎月の稼働実績を Web ページ等で確認可能なこと。
- (3) 機構が保持する DNS サーバの MX レコードを書き換えることにより不審メール対策サービスを利用可能とすること。
- (4) メールを受信配送経路について STARTTLS に対応した暗号化が可能なこと。
- (5) 送信者ドメイン認証 (SPF、DKIM、DMARC) に関する受信時の確認が可能なこと。
- (6) 実在するメールアドレスを登録することで、存在しないメールアドレス宛のメールを拒否可能なこと。
- (7) スパム対策エンジンを用いた不審メール対策を行うこと。
- (8) サービスを通過するメールに対する処理ポリシーを定義可能で、以下に示す処理を複数組み合わせる処理することが可能なこと。また、各処理の実行時には、指定したメールアドレスへの通知や件名・ヘッダ情報の追加/削除が可能なこと。
 - ・差出人、あて先メールアドレスによる隔離・受信許可/拒否、破棄
 - ・送信元 IP アドレスによる隔離・受信許可/拒否、破棄
 - ・送信者ドメインによる隔離・受信許可/拒否、破棄
 - ・メールの添付ファイル名、ファイル形式、ファイル数、暗号化 zip ファイルによる隔離・受信許可/拒否、破棄
 - ・メールヘッダ、本文に対するキーワードによる隔離・受信許可/拒否、破棄
 - ・メールサイズによる隔離・受信許可/拒否、破棄
 - ・送信者ドメインの認証結果による隔離・受信許可/拒否、破棄
 - ・アドレスフィルタ（差出人、あて先）、IP アドレスフィルタ、送信ドメイン認証フィルタが存在すること。
 - ・メールの添付ファイルに対してサンドボックスで解析できること
- (9) 不審メールに対する隔離対策が可能であり、隔離通知を受信者に通知可能であること。
なお、ユーザ毎に隔離フォルダを有効にした場合、ユーザ自身で受信を拒否あるいは許可したいアドレス(ブロックリスト及びセーフリスト)の設定が可能であること
- (10) 隔離されたメールは 14 日以上保存可能とし、その期間を経過したのちに隔離メールが残っている場合は自動的に削除すること。
- (11) 隔離されたメールは、宛先アドレスまたは指定したアドレスにレポートメールとして通知可能なこと。なお、隔離レポートは送信日時を指定して定期的に通知可能なこと。
- (12) 管理者画面において、不審メール対策サービスに関する Syslog 情報として、ポリシ

ーで処理したメールに関するログ、システムに関する操作ログ、SMTP 処理のログを閲覧およびダウンロード可能なこと。なお、Syslog 情報は機構が保持する Syslog サーバへの転送が可能であること。

(13) 管理者画面は、統計情報として、以下の項目を閲覧可能なこと。

- ・メール総受信数、30 分当たりのメール受信数、その際の帯域幅
- ・ポリシー毎の処理内訳
- ・メール受信者の受信数の TopN
- ・隔離メールの管理情報(ユーザ単位の隔離、システム単位での隔離)
- ・受信件数上位のユーザ毎の統計情報
- ・IP セッションの表示

(14) 管理者画面において、管理者及びユーザ毎隔離画面にアクセス可能なユーザを定義可能なこと。また、定義したユーザのアクセス権限を管理可能なこと。

(15) REST API 機能を有していること。

(16) 特定のファイルに対するマクロ除去機能を有し、添付ファイルからマクロを除去・添付ファイルを削除してメール本文のみ・件名にタグ付け、のいずれかの方法でメールを配送可能なこと。

3.2.4 技術・障害等相談窓口

(1) 技術的及び障害時にメール及び電話が可能な問い合わせ窓口を設けること。なお、窓口は平日の 9 時から 17 時まで対応可能とすること。

上記について、チケット制とする場合は、サービス利用期間中に 30 チケット以上とすること。

(2) 不審メール対策サービスにおいて誤判定されたメールについて申告する窓口を設けること。

3.2.5 サプライチェーン・リスクに関する要件

(1) 受注者の資本関係・役員の情報、本契約の実施場所、従事者の所属・専門性(情報セキュリティに係る資格・研修等)・業務経験及び国籍についての情報を記した書類を、原子力機構契約締結後速やかに、原子力機構に提出すること。なお、提出した内容に変更が生じた場合は、その都度提出すること。

(2) 候補となるサービス等についてはあらかじめ原子力機構にリストを提出し、原子力機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、原子力機構と迅速かつ密接に連携し提案の見直しを図ること。

(3) 本件で必要となる受注者にて準備する機器等がある場合には、あらかじめ原子力機構に機器等リストを提出し、原子力機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、原子力機構と迅速かつ密接に連携し機器の見直しを図ること。

(4) 受注者が本件の運用設計、設定作業を行うにあたり、原子力機構の意図しない変更

や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。ISO9001 又は JIS-Q9001 の認証書類の提出でも可とする。

3.2.6 現行サービスからの移行に関する要件

本サービスを導入するにあたり、現行の不審メール対策サービスと異なるサービスを利用する場合は、移行作業にかかる期間・費用を考慮して対応すること。移行作業を実施するにあたっては、作業工程表及び導入パラメータ表を作成し、機構担当者の確認を得ること。また、作業完了後には作業報告書を作成すること。なお、現行の不審メール対策システムに関する詳細情報は、本契約の受注者にのみ開示する。

4. 納期

令和 7 年 10 月 1 日

(サービス利用期間：令和 7 年 10 月 1 日から令和 8 年 9 月 30 日)

5. 納入場所及び納入条件

茨城県那珂郡東海村大字白方 2-4

日本原子力研究開発機構 原子力科学研究所

情報交流棟南ウィング

システム計算科学センター サイバーセキュリティ統括室

6. 提出資料

本件に係る成果物について、次に掲げるものを紙媒体で 1 部及び電子媒体で 1 部納品すること。尚、カラーを使用する場合は、白黒でも印刷できるよう配慮すること。

No.	名称	提出期限	区分
1	資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修等）・実績及び国籍	契約締結日から二週間後	通知
2	業務責任体制（統括責任者名、総括責任者代理名、業務担当者名、業務担当者の実績・保有資格、統括責任者と業務担当者の役割分担、機構との連絡体制）	契約締結日から二週間後	通知
3	ライセンス証書	契約締結後速やかに	確認
4	作業工程表	作業二週間前	確認
5	導入パラメータ表	作業二週間前	確認
6	作業報告書	作業後速やかに	
7	検査要領書	作業二週間前	
8	検査成績書	作業完了後速やかに	

※印刷枚数の多い資料については電子媒体での納品のみとする。

※No4～8 は、移行作業を実施する場合には作成するものとする。

7. 検査

(1) ライセンスに関する検査

「6. 提出資料」の No3 に示すライセンス証書に基づき員数検査を実施する。

(2) 移行作業に関する検査（移行作業実施時）

「6. 提出資料」No7 に示す検査要領書に基づき「3.2.6 初期導入作業に関する要件」に示す初期導入作業完了後に機能検査を実施する。

8. 検収条件

「6. 提出資料」の納品及び「7. 検査」に合格したことをもって検収する。

9. 保証

サービス利用期間中に受注者に帰すべき設計上及び施工上の瑕疵が発見された場合は、無償にて速やかに保障あるいは良品と交換するものとする。

10. 守秘義務

受注者は、本業務の実施により知りえた情報を当機構に無断で第三者に漏えいしてはならない。

11. 情報セキュリティの強化

情報セキュリティの強化に係る取り扱いについては、別紙 1「情報セキュリティ強化に係る特約条項」に定められたとおりとする。

12. グリーン購入法

(1) 本契約において、グリーン購入法(国等による環境物品等の調達の推進等に関する法律)に適用する環境物品(事務用品、OA 機器等が発生する場合)の採用が可能な場合は、これを採用するものとする。

(2) 本仕様に定める提出書類(納入印刷物)については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

13. 疑義

本仕様書に関して、あるいは、記載のない事項については疑義が発生した場合は、当機構及び受注者双方協議の上対処するものとする。

以上

情報セキュリティ強化に係る特約条項

受注者（以下「乙」という。）は、本契約の履行に当たり、情報セキュリティの強化のため、契約条項記載の情報セキュリティに係る遵守事項に加え、以下に特約する内容を遵守するものとする。

（情報セキュリティインシデント発生時の対処方法及び報告手順）

第1条 乙は、情報セキュリティインシデントが発生した際の対処方法（受注業務を一時中断することを含む。）及び発注者（以下「甲」という。）に報告する手順について整備しておかなければならない。

（情報セキュリティ強化のための遵守事項）

第2条 乙は、次の各号に掲げる事項を遵守するほか、甲の情報セキュリティ強化のために、甲が必要な指示を行ったときは、その指示に従わなければならない。

- (1) この契約の業務を実施する場所を、情報セキュリティを確保できる場所に限定し、それ以外の場所で作業をさせないこと。
- (2) 業務担当者に遵守すべき情報セキュリティ対策について教育・訓練等を受講させるとともに、業務担当者には甲の情報セキュリティ確保に不断に取り組み、甲の情報及び情報システムの保護に危険を及ぼす行為をしないよう誓約させること。また、業務担当者の異動・退職等の際には異動・退職後も守秘義務を負うことを誓約させ、これを遵守させること。
- (3) 暗号化を要する場合は、「電子政府推奨暗号リスト」に記載された暗号化方式を実装し、暗号鍵を適切に管理すること。
- (4) 甲の承諾のない限り、この契約に関して知り得た情報を受注した業務の遂行以外の目的で利用しないこと。
- (5) 甲が提供する情報を取り扱う情報システムへの不正アクセスを検知・抑止するために、ログを取得・監視し全ての業務担当者についてシステム操作履歴を取得すること。
- (6) 甲が提供する情報を格納する装置、機器、記録媒体及び紙媒体について、業務担当者のみがアクセスできるよう施錠管理や入退室管理を行い、セキュアな記録媒体の使用や使用を想定しないUSBポートの無効化、機器等の廃棄時・再利用時のデータ抹消など想定外の情報利用を防止すること。
- (7) 情報システムの変更に係る検知機能やログ解析機能を実装し、外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時には、多要素主体認証を要求するとともに定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時の脆弱性対策を行うこと。

- (8) システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施するとともに、システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと。
- (9) 委任をし、又は下請負をさせた場合は、当該委任又は下請負を受けた者に対して、業務担当者が遵守すべき情報セキュリティ対策についての教育・訓練等を行うこと。
- (10) 契約条項に基づき甲が乙に対して行う情報セキュリティ対策の実施状況についての監査の結果、情報セキュリティ対策の履行が不十分である場合には、甲と協議の上改善を行い、甲の承諾を得ること。
- (11) 契約の履行期間を通じて前各号に示す情報セキュリティ対策が適切に実施されたことの報告を含む検収を受けること。また、本契約の履行に関し、甲から提供を受けた情報を含め、本契約において取り扱った情報の返却、廃棄又は抹消を行うこと。