

電力広域的運営推進機関
電子メール誤送信防止策の検討に係る業務委託
入札仕様書

電力広域的運営推進機関

平成 29 年 4 月 19 日

1 件名

電子メール誤送信防止策の検討に係る業務委託

2 調達の背景

電力広域的運営推進機関（以下「本機関」という。）では、電気事業法の定めに基づき、電気事業者からの需給計画・系統計画の取りまとめを行う等の役割を担っており、これらの業務の実施に関連して事業者から窓口担当者の個人情報を取得し、電子メールを利用して、各種連絡・調整や情報の交換等を行っている。

こうした中、昨年4月、一部の業務の実施にともない、複数の事業者に連絡のための情報をメールで送信した際、宛先をBCCに含めるべきところを誤ってTOとしたことにより、メールアドレス等を含む50名の個人情報が漏えいする事案が発生した。事案の発生を受けて、本機関では、全役職員に対して、複数事業者へメールを送信する際はBCC送信することを必須とし、送信する場合はダブルチェック（複数人での確認作業）することの周知を行ったが、その後、12月にも同様の事案が発生し、12名の個人情報が漏洩した。

本機関では、引き続き、ダブルチェックの実施の周知及び情報セキュリティ自己点検を通じた対策の実施状況の確認等の組織的・人的な対策を行っているが、人的統制に依存しているため、電子メールの誤送信に起因するリスクの発生の可能性を排除することができておらず、これに対応することが課題である。

このような背景から、監督官庁等の要求を踏まえ、情報セキュリティに及びプライバシーリスクマネジメントに知見を有する専門家の支援を得るための公募を行うに至った。

3 目的及び期待する効果

3.1 目的

電子メールの誤送信に起因する個人情報漏洩を防止するために有効な管理策を検討すること。

3.2 期待する効果

管理策の検討に当たっては、業務への負荷を必要最小限としつつ、予算の範囲内で最大限の効果を生み出すことができるよう効率的かつ効果的な実施方式とすることが求められる。

4 業務委託内容

4.1 対象範囲

電子メールの誤送信に起因する個人情報漏洩のリスクを対象とする。

4.2 アプローチ

本委託業務では、情報セキュリティに関するリスクマネジメントの指針をまとめた国際規格である「ISO/IEC27005:2011 情報技術－セキュリティ技術－情報セキュリティリスクマ

ネジメント」を参照モデルとして、図1に示す情報セキュリティのリスクマネジメントプロセスに沿って実施することを想定する。

(1) 組織状況の確定

本機関の情報セキュリティ関連規程及び関連資料の査閲、また利用者等へのインタビュー等により評価対象となる電子メールの利用状況を把握する。

(2) リスク特定

評価対象範囲における電子メールの誤送信に起因するプライバシーリスクを洗い出し網羅的なリスクの一覧を作成する。

(3) リスク分析

必要とされるリスク対応を検討するため、特定したリスクの業務への影響度や発生可能性等を分析する。

(4) リスク評価

分析した影響度、発生可能性に応じて、特に優先的に対応すべきリスクについて、関連法令やガイドライン等の規定体系を参照し、必要なリスク管理策を検討する。

(5) リスク対応

検討したリスク管理策を再発防止策報告書として文書化する。

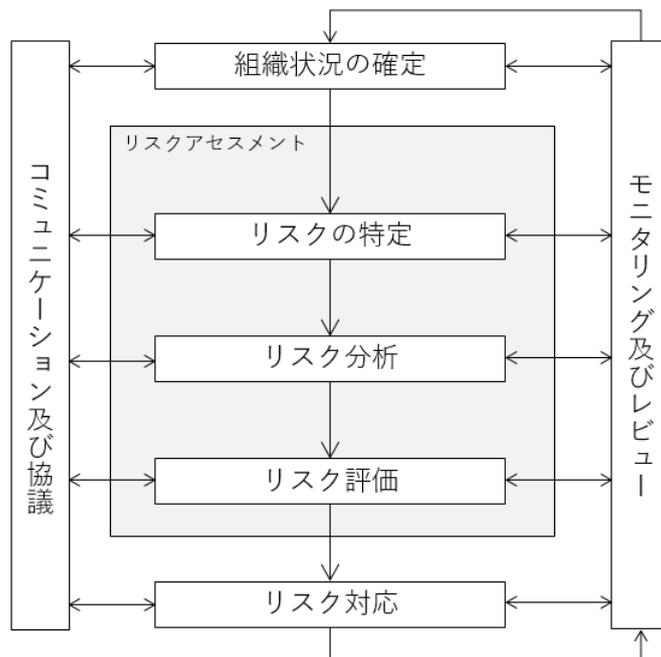


図1：情報セキュリティのリスクマネジメントプロセス

4.3 実施スケジュール

本業務委託の実施スケジュールの想定は、図2のとおり。

タスク	W 1				W 2				W 3				W 4			
組織状況の確定																
キックオフ	■															
組織状況の確定		■	■	■												
リスクアセスメント																
リスク特定					■	■	■									
リスク分析							■	■	■							
リスク評価									■	■	■					
リスク対応																
リスク対応											■	■	■	■	■	■

図 2：実施スケジュール

4.4 契約期間

契約開始から平成 29 年 6 月 30 日

4.5 成果物

受託者は以下の資料を作成・提出すること。

- 再発防止策報告書
- 再発防止策報告書の概要説明資料

5 実施体制

本業務の目的を理解したうえで、受託者にて最適な体制を構築するものとする。

なお、業務を実行するにあたり、選任するものは、政府機関の情報セキュリティ対策のための統一基準群について理解し、プライバシー影響評価等の関連業務の経験及び次のいずれかの資格を有する者であること。

- 情報処理推進機構の実施する情報処理技術者試験のプロジェクトマネージャー試験の合格者
- プロジェクト・マネジメント協会が認定する PMP (Project Management Professional) の資格保有者
- 情報処理推進機構の実施する情報処理技術者試験の情報セキュリティスペシャリスト試験の合格者
- システム監査技術者 (SA : Systems Auditor)
- 公認情報システム監査人 (CISA : Certified Information Systems Auditor)
- 公認システム監査人 (CSA : Certified Systems Auditor)

6 完了期限

平成 29 年 6 月 30 日

7 納入場所

電力広域的運営推進機関 事務所（総務部）

8 その他

- ① 本業務について、作業場所や作業端末等は受託者にて確保するものとする。
- ② 本仕様書に記載の事項は、本入札のために限り使用することとし、目的外使用や第三者への漏えいをしないこと。
- ③ この仕様書に定めのない事項について必要のある時は、委託者と受託者が都度協議し、決定するものとする。

以 上