# 通信機器製造会社Ａ社におけるＩＴ組織の役割・責任に関する監査

## 1. ＩＴ組織の現状の体制及び役割・責任の概要と影響を及ぼすＩＴ環境の変化

### 1. １．ＩＴサービスの概要

Ａ社は通信機器製造会社である。Ａ社の情報システムは製造部が利用する製造管理システム、営業部が利用する販売管理システム、全ての社員が利用するポータルシステムから成る。これら情報システムはオンプレミスで運用され、情報システム部が運用保守をしている。また販売管理システムにはインターネット販売システムが包含されている。インターネット販売システムはＡ社社員の他に法人や個人が利用しており、彼らの個人情報を蓄積しているため、情報セキュリティ対策を行う必要がある。

### １．２．影響を及ぼすＩＴ環境の変化

Ａ社経営陣はコスト削減を目的としてオンプレミスで運用している情報システムを、パブリッククラウドの外部サービスに移行することに決定した。これに伴い情報システム部が情報システムの移行の計画や、パブリッククラウド業者の選定に着手した。

本システム移行は着手してから３か月経過しており、システム移行計画やパブリッククラウド選定も進んでいることから、監査部はＩＴ組織の役割・責任の変更に関して監査を行うことにした。

## ２．ＩＴ組織の役割・責任の変更及び新たに発生するリスク

### ２．１．ＩＴ組織の役割・責任の変更

Ａ社の情報システムはオンプレミスで運用されている。現状、情報システムはサーバ、ＯＳ、アプリケーション全てを情報システム部が運用保守していたが、パブリッククラウド業者がサーバを、情報システム部がＯＳ、アプリケーションをそれぞれ運用保守することになる。情報システム部はＩＴ組織の役割・責任の変更として、運用保守要員の減る一方、パブリッククラウド業者の管理が追加された。製造部、営業部、その他の社員においてはＩＴ組織の役割・責任の変更はない。これはＡ社の情報システムがＷｅｂシステムとなっており、パブリッククラウドサービスの形態に移行し易いからである。

### ２．２．新たに発生するリスク

ＩＴ組織の役割・責任の変更に伴い新たに発生するリスクは次の通りである。

#### （１）情報漏えいの対処が遅れてしまうリスク

Ａ社の現状の情報システムはオンプレミスで運用されているため、情報漏えいインシデントが発生してもＡ社社員によって速やかに対応できる。それに比べ、パブリッククラウドサービスを利用する制約により情報漏えいの対処が遅れてしまうリスクが考えられる。

#### （２）パブリッククラウド業者の経営が悪化し業務が継続できなくなるリスク

パブリッククラウド業者の経営が悪化し、サービスが利用できなくなり、Ａ社の業務が継続できなくなるリスクが考えられる。

#### （３）サーバやネットワークの障害が発生し業務が継続できなくなるリスク

サーバやネットワークの障害が発生した場合、パブリッククラウドサービスを利用する制約により、速やかに障害対応することができず、Ａ社の業務が継続できなくなるリスクが考えられる。

以上の３つが、ＩＴ組織の役割・責任の変更に伴い新たに発生するリスクである。

## ３．新たに発生するリスクに対するコントロールと監査手続及び留意事項

### ３．１．新たに発生するリスクに対するコントロール

ＩＴ組織の役割・責任の変更に伴い新たに発生するリスクに対するコントロールは次の通りである。

#### （１）情報漏えいの対処が遅れてしまうリスク

情報漏えいの対処が遅れてしまうリスクに対するコントロールとしては、パブリッククラウドサービスが提供する運用監視ツールについて、Ａ社運用保守要員が精通し、情報漏えいインシデントを早期に発見するようにすることが、有効であると考えた。

#### （２）パブリッククラウド業者の経営が悪化し業務が継続できなくなるリスク

パブリッククラウド業者の経営が悪化し業務が継続できなくなるリスク対するコントロールとしては、パブリッククラウド業者のユーザ獲得件数の推移や財務状況を把握し、経営が悪化する兆候を察知して対処することが有効であると考えられる。

#### （３）サーバやネットワークの障害が発生し業務が継続できなくなるリスク

サーバやネットワークの障害が発生し業務が継続できなくなるリスクに対するコントロールは情報漏えいの対処と同様であるため割愛する。

### ３．２．監査手続及び留意事項

新たに発生するリスクに対するコントロールの有無について確認する監査手続及び留意事項は次のとおりである。

**（１）情報漏えいの対処が遅れてしまうリスク**

情報漏えいの対処が遅れてしまうリスクに対するコントロールの有無を確認する監査手続はシステム移行計画や補足資料を閲覧し、パブリッククラウドサービスが提供する運用監視ツールについて、 Ａ社運用保守要員が精通するため、十分な要員数と期間を確保することが計画されているかを示す監査証拠を得る、である。また留意事項として、パブリッククラウド業者が提供する運用監視ツールの支援サービスや問合せ対応が充実しているかについても確認する。

**（２）パブリッククラウド業者の経営が悪化し業務が継続できなくなるリスク**

パブリッククラウド業者の経営が悪化し業務が継続できなくなるリスク対するコントロールの有無を確認する監査手続は情報システム部長にインタビューし、ＩＴ組織の役割・責任の変更に伴いパブリッククラウド業者を管理する立場で、主体的にユーザ獲得件数の推移や財務状況を定期的に入手することが検討されているかを確認する。また留意事項として、万が一当該パブリッククラウド業者の経営が悪化する兆候を察知した場合の対策についても、検討しているかどうか確認する。

**（３）サーバやネットワークの障害が発生し業務が継続できなくなるリスク**

サーバやネットワークの障害が発生し業務が継続できなくなるリスクに対するコントロールの有無を確認する監査手続は情報漏えいの対処と同様であるため割愛する。

以上