演習１４　監査実施（２）

演習１２で作成した監査計画書、及び演習１３で作成した営業部内部監査の不適合報告書に基づき、S サービス株式会社の内部監査報告書を作成します。今回は、課単位の監査報告書とし、各課単位での改善活動を図ることにしました。

演習１４－１．　営業部・IT 構築サポート課の内部監査報告書を作成します。内部監査報告書の空欄を埋めてみてください。

内部監査報告書

文書番号：ISMS-監査-10-002
作成：平成３０年１１月３０日
承認：監査責任者（総務部長）
作成：営業部監査担当（総務部 システム管理者）

（１）導入区分

演習 14-1-1.　内部監査の導入区分について記述してください。

■監査期日

2006/10/20 - 10/22（詳細は添付したスケジュールを参照）

■監査目的

受託内容および受託データ、契約上の要求事項および個人情報保護を含む法規制上の要求事項を守るため、営業部において ISMS を導入する目的である仕組みの構築、運用、見直し、改善のうち、運用が適切に行われているかどうかを確認

■監査範囲

営業部 宣伝課
営業部 IT 構築サポート課

■監査基準

・情報セキュリティ基本方針及び社内ルール
・JIS Q 27001:2006 附属書 A

■監査チーム

リーダー：総務部　山田
メンバー：総務部　鈴木、加藤、井上

■被監査責任者

営業部・IT サポート課　川上課長

（2）概要区分

演習 14-1-2.　内部監査の概要区分について記述してください。

■結果概要

重大な不適合　1　件、軽微な不適合　0　件、改善の機会　3　件

■指摘内容

１．現地調査の被監査部門対象者へのインタビュー（A7.2.2）
「秘密」「極秘」「社外秘」とファイルボックスにラベルで分けられるべきであるが、実際にはラベル分けがされていない。

２．ヒアリングから（A7.1.1 / A7.1.2 / A7.1.3 / A7.2.1 / A7.2.2）
利用者端末の設定手順書でメールでのデータやり取りに関することの規定に関しての記録がない。
そのため資産目録に記載されておらず管理責任者が定められておらず、資産利用の許容範囲が文書化されておらず、分類の指針がなく、ラベル付けおよび組織の採用した分類体系による取り扱いが行われていない。

3. ヒアリング/現地調査から(A7.1.2)
組織内における情報の管理責任者について、証拠を得ることができなかった。

4.ヒアリング./現地調査から
資産利用の許容範囲に関する規則が文書化されているという証拠をえることができなかった。

■是正要求

1　件

演習 14-1-3.　内部監査の概要区分に記述すべき、充実点について記述してください。

■充実点

情報セキュリティ基本方針の周知、徹底は十分に実施されている。

（4）意見区分

演習 14-1-4.　内部監査の意見区分について記述してください。

■監査結論

3 点ほど運用の不備は見られたものの、全体的には ISMS の要求事項への整合性はほぼ適切であると考えられる。
検出された指摘事項については、広範囲に影響があると考えられるため、早急な対策が求められる。
なお、今回指摘した項目は基本的な項目であり、継続的に改善を行っていく必要がある。