TOSHO COMPUTER SYSTEMS Co.,Ltd

情報セキュリティ診断報告書

○○○○株式会社様

東証コンピュータシステム
リスクマネジメント室
情報セキュリティスペシャリスト/CISSP 菅原昭伸

2015 年 10 月 26 日

株式会社　○○○○○　御中

㈱東証コンピュータシステム

情報セキュリティ診断結果

1.

（１）診断対象

貴社の○○業界向けのシステムである○○○○システムの保守・運用業務

（２）診断目的

上記システムの情報セキュリティにまつわるリスクに対するコントロールが、リスクアセスメントに基づいて適切に整備・運用されていることを確認すること。

（３）利用した管理基準

JIS Q 27001

（４）診断概要

診断期間:2015 年 10 月 19 日～23 日

ヒヤリング対象者：総合管理部　Ｔ部長、Ｍ課長
システム管理部　Ｋ部長、Ｆ課長

（５）最終報告

報告日：2015 年 10 月 26 日

報告先：代表取締役社長　Ｎ社長

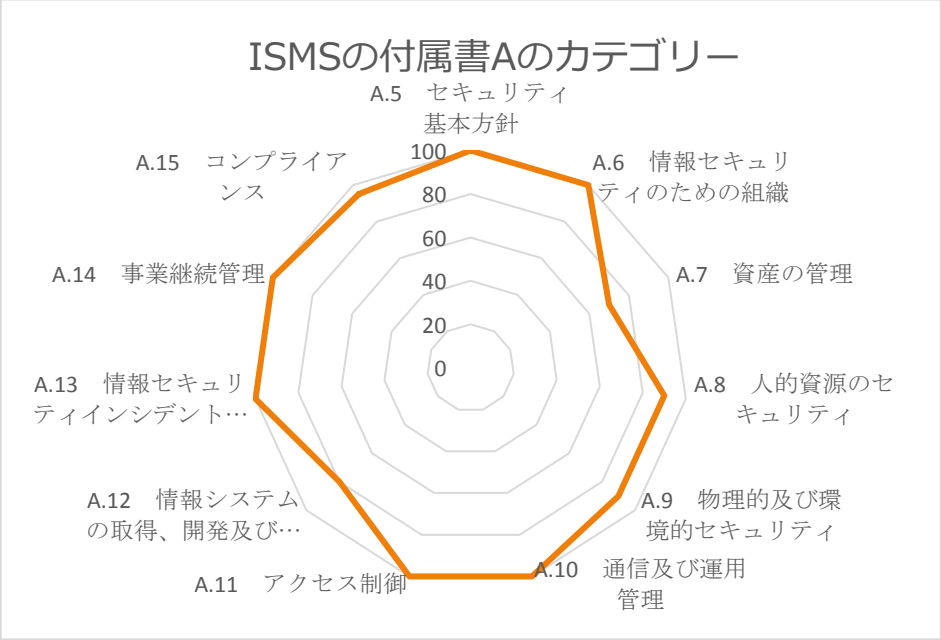
2. 総括

(1) 総合講評

○○○○システムがリスクアセスメントに基づき、概ね適切に、整備・運用されていることを確認しました。

下図に、今回の診断結果を評点化し、ISMS 付属書 A のカテゴリー毎に集計した結果を示します。(不備事項が発見されるごとに、減点法を採用)

全体に概ね良好ですが、A7.資産の管理の項目で、一部改善すべき項目が発見されました。（詳細は後述）。



3. 個別改善事項

(1) 文書管理に関する規程が存在しない

文書の機密性の尺度と、それぞれの表示方法や保管方法について定めたルール（例えば、このレベルの文書は関係者外秘とし、社内の人間でもアクセスできる者を制限し、かつ文書にはその旨を記し、施錠管理を行う、といったルール）が存在しません。現状のままだと、万一漏えいした時に、不正競争防止法でいう営業秘密（秘密管理性と有用性と非公知性の三点が要件。一般に裁判では秘密管理性で争われることが多い）として認められない可能性が大です。秘密管理性とは、情報の種類、性質、管理の方法・態様、情報を保有する事業者と情報にアクセスした者との具体的な関係等の諸般の事情に照らし、客観的にみて、情報にアクセスした者において当該情報が秘密情報であることを認識し得る程度に管理されていることを要するものと解される、とされています（添付の知的財産権判例ニュースを参照のこと）。

(2) 入館証の ID カードを紛失したときの失効手続きに関する規程がない

入退館要領によると、紛失時の入館証の再発行に関する記載があります。ただし、紛失時に最も心配すべきは、入館証を取得した第三者が、不正に入館証を利用し、建物や部屋に入り、情報資産等を盗み出すことです。従って、入館証を紛失したと気付いた時は、まず管理者に連絡し、その入館証で他人が入館できなくすることが第一だと考えます。入退館要領に紛失時に速やかに失効手続きを実施することにについて追記すべきです。

(3) セキュリティ教育の実施について

今年度のセキュリティ教育が当初の計画通りに実施されていません。担当者が長期病欠のためとお聞きしましたが、セキュリティに関する教育は繰り返ししかありません。代わりのセキュリティ教育の担当者を指名したうえで、確実な実施をお願いします。

(4) ソフトウェアの管理台帳が整備されていない部署がありました。