

< 報告 (5) >

あいち電子自治体推進協議会 情報セキュリティ監査報告書

平成 1 8 年 2 月 2 0 日

あいち電子自治体推進協議会
情報セキュリティ監査統括責任者 殿

監査人名

A班: 赤坂義宏 (日進市市長公室市民交流課)
鈴木 海 (東郷町町長公室企画情報課)
石原恒義 (美和町総務部企画課)
江口智広 (常滑市企画部企画課)
河田 明 (東海市企画部情報課)
B班: 相木直人 (大府市企画政策部情報推進課)
高島秀和 (岡崎市企画政策部IT推進課)
杉浦浩司 (碧南市総務部行政情報課)
丹羽康人 (刈谷市企画部情報システム課)
浅倉淳志 (豊橋市総務部情報システム課)
尾崎弘章 (蒲郡市企画部情報ネットワークセンター)

平成 1 7 年度あいち電子自治体推進協議会情報セキュリティ監査について (報告)
このことについて、「あいち電子自治体推進協議会情報セキュリティ管理基準」に照らし、平成 1 7 年 4 月 1 日から平成 1 7 年 1 2 月 3 1 日までの期間に係る、あいち電子自治体推進協議会 (以下、「協議会」という。) の情報セキュリティ対策の実施状況について監査を実施しました。

この監査は、情報セキュリティに関わるリスクのマネジメントが効率的に実施されるよう、リスクアセスメントに基づいた対策がとられているかを確認して、問題点を提示するといった観点から実施したものであり、下記のとおり監査結果を報告いたします。

記

1 総 括

「地方公共団体情報セキュリティ管理基準」を参考に、「あいち電子自治体推進協議会情報セキュリティ管理基準」(以下、「セキュリティ管理基準」という。) を作成し、セキュリティ対策のため特に重要と思われる項目 (セルフチェック項目) を抽出し、協議会のセキュリティ対策に関する管理状況の確認を実施しました。

セキュリティ対策が実施されているかどうかの判断は、「実施されている」、「実施されていない」の または × としたため、協議会事務局担当者へのインタビューにより、現にセキュリティ対策が運用、実施されていることが確認できたとしても、文書化 (実施手順、規定類の整備) を求めているセキュリティ要求事項であれば、文書化されていない場合は「実施されていない」との判定をしました。

今回の管理状況実施確認では、現にセキュリティ対策が実施されているにもかかわらずその実施手順等が文書化されていない状況が数多く見られました。そのため、協議会の今後のセキュリティ対策に関する課題の一つとして、実施手順、計画書、規程類等の整備をあげさせていただきます。

なお、監査結果の詳細については、「12 監査結果 (1) から (4)」のとおりとりまとめました。

2 監 査 人

協議会情報セキュリティ研究会 (情報セキュリティ監査グループ)

3 監 査 目 的

協議会の情報セキュリティ対策に関する助言を行うことを目的として実施しました。

- 4 監 査 種 別
内部監査
- 5 実 施 日
平成18年2月9日 午前11時～午後6時
- 6 実 施 場 所
愛知県自治センター 9階 システム設計室
- 7 監 査 対 象
(1) 協議会事務局情報セキュリティ担当者及び情報システム担当者
(2) 協議会が運用する電子申請届出システム
なお、現在協議会が運用するシステムは、協議会Web、電子申請届出システムがありますが、より住民へ影響を与える電子申請届出システムを今回の監査対象としました。
- 8 監査対象期間
平成17年4月1日から平成17年12月31日
- 9 監 査 基 準
(1) セキュリティ管理基準
(2) セキュリティ管理基準から基本的な項目又は優先度の高い項目として258のサブコントロール(管理状況)を抽出し、チェック項目として設定しました。
- 10 監 査 手 法 ()
上記 9 - (2) のセキュリティ管理基準から抽出した258項目のサブコントロール(管理状況)の実施状況を、レビュー及びインタビューにより確認しました。
- 11 評 価 方 法
(1) 実施指数を用いた評価方法を用いました。
(2) サブコントロール(管理状況)が整備・運用されているかの判断基準は、実施できていない、実施できている、のいずれかで判断しました。(判断基準 別添2)
- 12 監 査 結 果
(1) 管理基準実施チェック表
(2) 管理基準実施チェック表(集計)
(3) マネジメント領域に基づくレーダチャート
(4) 258項目のサブコントロール(管理状況)に基づくレーダチャート

診断結果については、セキュリティ確保のため、
会員外非公開とさせていただきます。

- 13 その他特記事項
データセンター運用管理者により、あいち自治体データセンターにおける全システムでセキュリティ診断が実施され、報告書が作成されているため、今回の監査では技術的診断は実施しておりません。

() 監査手法について

- | | |
|---------|-------------------------|
| ・インタビュー | インタビュー形式で質問し実態を把握する方法 |
| ・レビュー | 文書類を入手してその内容を調べる方法 |
| ・視察 | 業務を行なっている状況を見て実態を把握する方法 |
| ・質問書 | 質問書に記入してもらい実態を把握する方法 |
| ・ログ分析 | 情報システムに記録されたログを分析する方法 |