

情報セキュリティ外部監査報告書

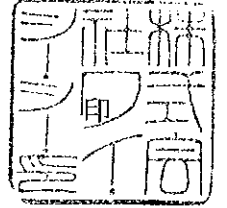
平成17年3月23日

日野市

情報セキュリティ統括責任者

河内 久男 様

株式会社ワイ・シー・シー



弊社は、「ISMS 認証基準 (Ver2.0)」「日野市情報セキュリティポリシー」及び「地方公共団体情報セキュリティ管理基準」(以下「監査基準」という)に照らして、2005年2月16日から2005年3月14日までの期間に係る「市民部市民窓口課」「市民部七生支所」及び「総務部情報システム課」にて運用されている「J-NET(住民基本台帳ネットワークシステム)」「MindCity(住民基本台帳事務システム)」及び「公的個人認証」の各業務を対象として、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た。弊社の任務は、監査手続きを実施した結果に基づいて助言をおこなうことにある。

弊社の監査は「監査基準」に準拠しておこなわれた。監査は、情報セキュリティに係わるリスクのマネジメントが効果的に実施されるよう適切なコントロールが採用されているか否かを確認、問題点を検出し提示するという観点からおこなわれている。

弊社のおこなった監査の実施状況について「監査基準」に照らして、以下の「情報セキュリティ外部監査報告書」として別紙の通り報告する。

日野市様に於いては、「日野市情報セキュリティポリシー（日野市情報セキュリティ基本方針及び同対策基準）」策定後、最初の外部監査であるため、監査は「日野市情報セキュリティポリシー」の策定内容、浸透及び遵守状況の確認をポイントとしておこなった。

監査は、監査基準（「ISMS 認証基準（Ver2.0）」、「日野市情報セキュリティポリシー」及び「地方公共団体における情報セキュリティ監査の在り方に関する調査研究報告書 別添 1 地方公共団体情報セキュリティ管理基準」）に基づきおこなった。対象部門に調査票を配布し、状況確認を行い回収後、各部門に対しヒアリング調査をおこなった。ヒアリング調査はサンプリングでおこない、部門への立ち入り調査もあわせておこなった。

「日野市情報セキュリティポリシー」策定の手続き、浸透状況については特に重要な問題点は検出されなかった。ただし、リスクマネジメントが不十分である箇所が検出された。

各組織の「情報管理者」「セキュリティリーダー」の意識は高く、情報セキュリティに対する対策の実施はおこなわれているが、全ての職員が同じ行動を取れる仕組みを確立する必要性を感じた。

総論的に言って、「日野市情報セキュリティポリシー」は高いレベルで浸透し、個々のセキュリティ管理策は効果的に実施されているが

- 対象となる情報資産に対する「脅威」、「脆弱性」を加味したリスク分析
- リスク分析に基づくリスクマネジメント
- リスクマネジメントに基づく管理策策定

を体系付けて実施し、管理策策定の根拠を明確にした上で定期的なリスクマネジメントを実施し、より効果的な管理策の策定、運用をしていくことが望まれる。

なお、同時に実施した「住民基本台帳ネットワークシステム」、「公的個人認証システム」への監査については、個々のシステムに対して関係省庁にて策定された要求事項に基づくシステム運用規程、実施手順が存在し、その全てにおいて日野市情報セキュリティポリシーで要求されるセキュリティレベルを満たしていることを確認した。

また、「住民基本台帳事務システム」への監査については、関係省庁ならびに日野市情報セキュリティポリシーに基づく運用規程、実施手順が存在し、日野市情報セキュリティポリシーで要求されるセキュリティレベルを概ね満たしていることを確認した。