豊　中　市

ISMSの国際規格「ISO／IEC27001」の認証を全国の市町村で初めて取得

～市民が安心して暮らせるまちづくりをめざして～

背　景

近年、情報通信技術の急速な進展に伴い、大量の個人情報漏洩や情報システム障害などの事件・事故のニュースが毎日のように新聞を賑わしています。

一方、当市が平成14年度に実施した市民アンケートでは、「電子自治体を実現する上で大切なことは何ですか」という質問に『不正な侵入や個人情報の漏洩などに対する安全性を確保すること』との回答が全体の約７割を占める結果となり、個人情報の重要性が増大してきているとともに、情報セキュリティ問題への取り組み方を抜本的に強化する必要があると認識されてきています。

経　過

当市では、平成元年に「個人情報保護条例」の策定を行い、個人情報保護に積極的に取り組んできました。平成15年には情報セキュリティポリシーを策定し、情報セキュリティの重要性の認識と知識を深めてもらうための研修などを実施するとともに、昨年には保護条例の全面改正を行い、罰則適用を拡大するなど一層の強化を図ってきました。

しかしながら、情報セキュリティ対策は、一部の職員が考え、それぞれの職員は決められたことをただ実行すればいいというものではなく、職員一人ひとりが情報セキュリティ対策を常に意識し、確実に実行し、さらには改善していける体制を確立していかなければなりません。

また、これらの取組を外部にＰＲすることにより、市民からの信用と信頼を得ることが重要であると考えました。

ＩＳＭＳ認証取得への取り組み

平成17年４月、「情報セキュリティマネジメントシステム（ＩＳＭＳ）」の認証取得に向けた取組を開始しました。

「ＩＳＭＳ」とは「Information Security Management System」の略で、「情報の安全を管理・運営するしくみ」のことです。

ＩＳＭＳでは、継続的な管理・運営のしくみとして、図１のような「ＰＤＣＡモデル」が採用されています。

では、ＩＳＭＳを導入するにあたり、本市において具体的にどのような活動を行ったのかを紹介していきます。

図１　ＰＤＣＡモデル

１．ＩＳＭＳの適用範囲の決定

個人情報の基礎となる「住民基本台帳」を取り扱う市民課、庄内、新千里両出張所、並びに「住民情報システム」を管理する情報政策室をＩＳＭＳ認証取得に向けた適用範囲とする部局に決定しました。

２．ＩＳＭＳの基本方針を策定

ＩＳＭＳを導入・運用するにあたり、既存のセキュリティポリシーでは足らなかったリスク分析や是正・予防処置の手法など要綱や手順などで補足しました。

３．情報資産の洗い出し

保護すべき情報資産について次の４つに分類して台帳を作成しました。

①情報・データ資産

データファイル、証明発行申請書、操作マニュアル　など

②ソフトウェア資産

業務用アプリケーション、開発用ツール　など

③物理資産

コンピュータ装置、磁気媒体、空調設備、電算施設　など

④サービス資産

オンラインシステム、保守サービス　など

また、洗い出した情報資産について、「機密性」「完全性」「可用性」の三要素の観点から資産価値を

決定しました。

4．リスクの分析・評価

災害や事故、不正アクセスなどの脅威の一覧表を作成し、情報資産がこれらの脅威に対して取られている対策を分析することにより情報資産の持つ脆弱性を評価しました。そして、資産価値、脅威の発生頻度、脆弱性から情報資産が抱えるリスクの大きさを決定しました。

5．リスク対応計画の実施

リスクが大きい情報資産について、リスク低減のための対策を計画し、実行しました。なお、ＩＳＭＳの認証規格には、物理的、人的又は環境的などの100を超える情報管理策が用意されており、実行する対策の計画はそれを参考に行います。また、これらの管理策について、適用の採否をまとめた「適用宣言書」を作成しました。

6．文書・記録類の整理

ＩＳＭＳの認証規格では、文書や記録の管理について細かく定義されています。必要な手順類を作成するとともに入退室などの記録類についても見直しや作成を行い、保管場所や保存年限を定めた一覧表を作成しました。

7．業務継続計画の作成、訓練の実施

事件・事故などが起こった場合でも、可能な限り業務を継続させることや、速やかに復旧させるための計画を作成しました。また、実際にその計画に基づいた訓練を行い、計画の有効性の評価も行いました。

8．教育・研修の実施

ＩＳＭＳの考え方、セキュリティの基本方針などを周知するための研修を行いました。また、専門家による内部監査の担当職員への研修も行っています。

9．内部監査の実施

研修を受けた職員により、ＩＳＭＳの活動が認証規格に沿って適切に行われているかを点検するための内部監査を実施しました。

10．経営陣によるレビュー

助役を筆頭とするセキュリティ会議を開催し、内部監査の結果、リスク分析の結果、ＩＳＭＳの構築の進捗状況などを報告し、今後の進め方などを議論しました。ＩＳＭＳでは、これをマネジメントレビューと呼びます。

11．審査機関による審査

基本方針、手順、記録類などが認証規格に沿って作られているかを確認する書類審査、及びその手順などに従って実際に業務が行われているかを確認する実地審査が認証機関の審査員により延べ６日間に渡り行われました。

こうして、平成18年６月１日付けで、ＩＳＭＳの国際認証規格である「ＩＳＯ／ＩＥＣ27001」の認証を取得しました。

ISO27001 IS503505のマーク


認証授与式

今後の展開

認証取得の目的は、情報セキュリティ対策の管理・運営について、国際的な規格に則った認証制度で認定されることにより、市民からの信頼感を一層高めるとともに、情報セキュリティ対策を全ての職員が理解した上で実行し、より良いものにしていく体制を作り上げていくことでした。

また、専門的な審査を毎年受けることにより、実施しているセキュリティ対策や運用が、本当に適切なものであるという安心感と自信を持って「仕事ができる」ことになります。

現在は、職員に対しＩＳＭＳとは何なのかを知ってもらうため、定期的に「ＩＳＭＳ通信」を発行しています。


「ＩＳＭＳ通信」のキャラクター

今後は、今回適用範囲とした部局において、さらに継続的な取り組みを進め、その中で得られたノウハウを他の部局にも展開することにより市全体のセキュリティ水準を向上させ、「安心の電子自治体づくり」を目指していきます。