

お客様情報の流出経緯と対策に関するご報告

会社名 株式会社ミロク情報サービス
代表者名 代表取締役社長 是枝周樹
(コード番号 9928 東証第2部)
問合せ先 経営管理本部長 滝本訓夫
(TEL . 03 - 5361 - 6369)

弊社高松支社管轄のお客様情報が流出する事故が発生し、お客様をはじめ関係各位に多大なるご迷惑やご心配をお掛けしましたことに対して、改めて深くお詫び申し上げます。

これまでの調査結果と今後の対策について、以下にご報告させていただきます。

1. 事実確認および事故の原因

(1) 経過

- ・インタ - ネット匿名掲示板に個人情報流出の記事を発見し、調査を開始しました。(10月25日)
- ・流出が事実である事を確認し、流出内容、流出原因、流出元の特定をすすめました。(同日)
- ・情報流出元が弊社社員の私用PCであること、流出した情報が弊社高松支社管轄のお客様の情報であることを確認しました。(10月26日)
- ・プレスリリース(東証適時開示)、原因への対策処置、全社緊急対策処置を実施しました。
- ・該当のお客様や当局、並びに関係諸団体への報告とお詫びを実施しました。
- ・社内の処分、再発防止策の検討を行いました。(～11月末)

(2) 事故の原因

弊社では、お客様情報を中心とした大切なデータは、サーバーに保管し、お客様情報取扱諸規定に基づき厳重に管理していました。今回の事故では一社員が諸規定に違反して、自宅で作業するために会社のサーバーから個人所有のUSBメモリーへお客様情報を取り出して自宅に持ち帰り、私用PCへコピーしておりました。当該PCにはファイル交換ソフトが組み込まれており、更に当該PCがウイルスに感染していたことによって、本人が意図せず外部に流出してしまいました。

2. 直接原因への対策(実施済)

(1) 事故対象PC等の処置

当該PC、USBメモリーからの会社データ削除、ファイル交換ソフトの削除および検疫とウイルス駆除を実施しました。

(2) 緊急予防処置

全社員に対して、PCやネットワークの使用ルールの再確認を実施しました。

全社員に対して、現状の情報資産のセキュリティの棚卸を実施しました。

(3) 社内の処分：諸規定に違反した社員及び管理責任者の処分を実施しました。

3. 弊社として取り組む予防処置(恒久対策)

弊社は、従来より、個人情報保護規定を制定し、社内通達、ガイドラインにて管理策を実施してまいりました。しかし、今回の事故調査結果を踏まえて全社的に情報管理体制の検証を行いました結果、現在、東京の営業部門のみで適用しているISMS(注)を早期に全国に拡大して情報管理策を実施する

ことで、全社的なセキュリティ・マネジメントの体制（P D C A）を強化することいたしました。経営者から現場の担当者までが実行すべき 133 項目の具体的な管理策を定めて遵守してまいります。

弊社は今回の事故を真摯に受け止め、経営者を筆頭に全社一丸となって今後の再発防止策に全力を尽くす所存でございます。何卒ご理解のほどお願い申し上げます。

【個人情報保護に関するお問い合わせ窓口】

株式会社 ミロク情報サービス 内部統制室 03-5361-7011（平日 9:00-17:00）

（注）I S M S（情報セキュリティマネジメントシステム）：組織が、情報セキュリティリスクを管理し、継続的にリスクの回避や軽減ができるマネジメントシステムをいいます。ISMSでは、組織が保護すべき情報資産について、Confidentiality(機密性)、Integrity(完全性)、Availability(可用性)(C I Aと総称)をバランスよく維持し改善していくこと(P D C A)が重要とされています。ISMS 認証基準の国際規格化(ISO/IEC 27001:2005)に伴い、JIS Q 27001 : 2006 認証としてJ I S化されています。