

Q&Aで学ぶ

本部・営業店に求められる 情報漏えい対策のポイント

昨今、情報管理の不備により顧客データが不正に利用される事件が頻発している。そこで本特別企画では、金融機関における情報管理の問題点や、求められる対策・体制整備などについて解説する。



Q1 金融機関で顧客情報 管理の厳格化が 求められている理由は？



平 成17年より施行されている「個人情報保護に関する法律」、いわゆる「個人情報保護法」を踏まえ、金融機関においても個人情報と顧客の情報管理は義務であり、コンプライアンス遵守の面からも重視されるところである。

金融庁においても、法・施行令・基本方針に則り、ガイドラインを策定している。まず、この背景を見てみよう。

個人情報の流出事故が増加

個人情報保護法の目的は、コンピュータや通信環境の高度化・進展に伴って、個人情報の利用が拡大していることから、その取扱いの正しさを方針を明らかにし、国や公共団体の責務、事業を行う企業の守るべき義務を決めることに

よって各個人の権利を守ることとされている。

昨今、個人情報の漏えい・流出事故が増え、詐欺事件などがニュースとして取り沙汰されたことで社会的な不安感が広がっている。また、平成19年より開始された公的機関での住民基本台帳ネットワークにより、自治体においても各団体を超えて住民データにアクセスが可能となったことで、便利になった反面、個人情報の安全管理が必須となった。

このような背景から、情報セキュリティ対策と名付けられた安全管理の措置が企業も含めて義務付けられたのである。

特に金融機関においては財産など慎重に扱うべき顧客情報があるため、より厳格な管理・運用が求められるといえる。

Q2 実際に金融機関では これまでどんな問題が 発生しているの？



あ る金融機関では、ATMの保守管理業務を再委託していたメンテナンス業者による事件が発生している。悪意を持つ内部関係者によるものである。

このケースでは、ATMの保守作業において、預金者のカード情報や暗証番号などを不正に入手して偽造カードを作成し、現金を不正に引き出すという刑事事件になっている。

原因としては、①再委託先の担当者が長年、同じ金融機関を担当していたことにより環境や事情に精通し、周囲の監視を含め、緩みがあったこと、②ATMの管理についての特権が広く与えられており、「取引履歴」「暗証番号」「ATM機器の管理」までも入手・実行できる状況にあったこと

挙げられる。

対策として、まず①は顧客情報の取扱いにおいては記録・ログを取り、その監視を確実に実施することが求められる。本ケースでいえば、メンテナンス作業において取引履歴や暗証番号の取得などが業務上必要であったのか、その頻度、回数は適切であったのかなどが監視によりチェックできた可能性がある。

監視においては、事前の作業内容の文書に基づく明確化と、実際の作業結果をログと照合することにより複層化し、多段階でのチェックや承認体制で慣行になりがちな業務の安全を確保できるといえる。また、その体制で業務を遂行するという環境自体が情報漏えい事故の抑制につながる。

漏えいによる損害賠償額は平均約4000万円と多額

次に②は、情報・データに対するアクセス権の制御が肝要である。「取引履歴」「その解析による暗証番号情報」「ATM機器の管理」と異なる情報に関する権限を複数持たせていたことにより、不正な情報入手と悪用が可能な状況であった。各業務を細分化し担当者に分けることにより権限を分散することで、個人やデータを特定できないようにしてリスク管理を行うことは、情報セキュリティでは重要なポイントになる。

反面、運用や管理においては煩雑となり、生産性の面からは非効率に見えるだろう。しかし、結果として事件になると、被害の保証

や顧客対応などで莫大な費用と時間を費やすこととなる。

NPO日本ネットワークセキュリティ協会の調べでは、個人情報漏えいインシデント(事件・事故)が起こった場合、平均の想定損害賠償額は1人あたりで5万円を超え、1件あたりでは約4000万円となっている。顧客情報を守ることは結果として、自組織や仕事自体を守ることにつながることを理解する必要があるだろう。

このほか、別の金融機関では、システム保守の再委託先従業員が事務センターでの保守作業時にサーバーからUSBメモリへ顧客データをコピーし、個人150万件、法人13万件的顧客情報が外部に持ち出される事件があった。現場の職員が必ず立会いを行うなど管理体制の強化が指示されている。

金融機関ではないが、今般、大手通信教育企業における過去最大規模の個人情報漏えい事件が起こった。このケースでも管理・運用体制の不備が指摘されており、形骸化されがちな運用ルールの再徹底、継続が重要である。