

平成 18 年 3 月

## 金融検査指摘事例集に見る営業店の顧客情報管理 - 態勢構築と事故防止

PwC アドバイザリー株式会社  
業務改善サービス部門  
パートナー 原 誠一

### (1) 情報管理と電子メール

多くの金融機関では、顧客情報の管理に関しては電子メールの取扱い規程が定められている。そのような規程の存在にもかかわらず、金融庁検査において、顧客情報や業務関係資料を自宅等へ送信している事例が指摘されている。

電子メールは、一度に大量の情報を多数の受信者に送信することが可能であるため、その取扱いは、顧客情報に限らず社内情報も含めルールを定め、守るための仕組みを構築する必要がある。ここでは、ID・パスワードによるアクセス制御、ウイルスチェック、機器の盗難・紛失対策などシステム共通の対策を前提とした上で、特に営業店での顧客情報の電子メールの取扱いに焦点を当てて説明する。

#### 業務目的外の電子メールの使用禁止

内部・外部不正防止の観点から業務目的外の電子メールの使用を禁止する必要がある。規程等で業務目的外の電子メールの使用を禁止している場合でも、実際には業務外で使用されていることは多いと思われる。より実効性を持たせるために電子メールの利用者を、必要最低限に限定し、メールアドレス付与時に業務外での利用禁止についての同意書をとることや、違反時についての罰則規定について形式的にならないように周知徹底する必要がある。また、遵守状況については、普段から送受信内容についてチェックするなど形式的な対応にならないようにすることが重要である。

#### 自宅等への転送の禁止

顧客情報ファイルを含んだメールを、自宅等の PC で作業を行うために個人所有のアドレスへ転送することは、紙の情報の持ち出し、持ち帰りと同様に管理される必要がある。

紙の情報の持ち出し、持ち帰りとは異なり、転送が容易であることに加えて、セキュリティレベルが比較的低い自宅等の PC は不正アクセスによる情報漏えいにつながり易いことから、個人所有のアドレスへの転送は禁止される必要がある。

また営業店で使用している端末から、WEB メールや BLOOMBERG 等の端末を介したメール機能など会社のメールシステム外から送受信できないか確認し、そのようなことが可能な場合には、当

該機能の使用を禁止するルールを制定し、本部の IT 部門に対し物理的にも利用ができないように設定を依頼する必要がある。

#### 送信時の取扱い

顧客情報を含んだ電子メールの送信時には、本文に顧客情報を載せるのではなく、添付可能ファイル形式 (ZIP、PDF 等ファイル形式に加え、変更・印刷の許可・不許可等のファイル内の設定等も含む) を定めた上で、パスワードを設定してから添付するなど、漏えい防止策を講じる必要がある。当然のことながらメールは暗号化してから送信を行い、パスワードも別途通知する。よく、パスワードがメール本文に添付ファイルと共に記載されていることがあるが、このような場合は、誤送信や不適切な転送が行われた場合に、効力を持たないため、必ず別途通知する旨を徹底する必要がある。

また添付する顧客情報については、社内の情報管理と整合した管理区分に基づき送信可能情報を限定し、必要に応じ送信前の承認プロセスを定める必要がある。

#### 記録とモニタリング

取り扱う情報の重要性の観点から、必要に応じて事前承認プロセスを定める必要があるが、全ての送信情報を事前に確認・承認することは、業務効率の観点から現実的とはいえない。

その場合でも、事後監査の観点に加え、漏えい事案等発生時の分析や訴訟時の証拠としての活用の上でも全ての送信情報について、改竄 (変更)・削除されない形で記録 (データとして保存) しておく必要がある。また、BCC による自動送信機能を利用した管理者への送信、メールフィルタリング機能等を利用し、疑わしいメールの事前確認・承認など、管理者による随時、定期的なモニタリングがなされる必要がある。

メールの記録とモニタリングは、基本的には不正使用を発見するための統制に分類されるが、当該措置が実施されているということを、職員に通知することで、不正使用の抑止力となり未然防止の効果も同時に発揮する。

#### 守らせるための人的管理措置

漏えい事案等を防止・管理する上では、組織としての仕組み (組織的安全管理措置)、技術面での仕組み (技術的安全管理措置) だけでなく、管理者・使用者に対する人的側面での仕組み (人的安全管理措置) についても整備することが重要である。

人的側面での仕組みは、現場である営業店における統制であり、多くの場合、この統制の実効性に問題があることから、不祥事件が発生している。

多くの職員は、電子メールの送受信のルールについて理解はしているが、業務量や送受信ルールの手順の煩雑さから、ルールを逸脱してしまうことが多い。そのような逸脱からすぐに不祥事件につながる可能性は低いことから、繰り返し行ううちに、逸脱に対する意識も希薄化してしまうことになり、やがて情報漏えいに発展することになる。

このような事態を回避するためには、ルールの逸脱を見逃さない、許さない環境を醸成する必要がある。そして、そのためには支店長席のリーダーシップが不可欠となる。

店内研修実施の際には、ルールの遵守は、自身を情報漏えい等の被害から守るものであり、ルールの逸脱が発覚した場合の処罰を厳格に適用することで、ルールの逸脱が割に合わないことを、担当者に実感させる必要がある。

また、メールの送受信記録の確認についても形式的なものとしないうために、業務日誌と照らし合わせるなど、不必要なメール送信がなされていないか業務の実態に即した確認も行う必要がある。

#### 守れる環境の醸成

自宅等へのメール送信の背景には、自宅で仕事をするという動機がある。仕事の持ち帰りは、多くの金融機関では原則禁止されているが、実態としてそれが遵守されているかは別問題である。そのような中では、仕事の持ち帰りについてあらためて禁止する旨を周知徹底するだけでなく、持ち帰りをしなくて済むような人員の配置や業務のサポート体制を再構築することも有効な対策となる。

## (2) FAX 送受信管理

金融庁検査指摘事例において、FAX の登録先確認や送信先への事前連絡が励行されていないことから、顧客の重要情報が含まれている文書等を誤って第三者に送付する事故が生じている例が挙げられている。

ここでは FAX 送受信に際して、想定される事象を整理し、それらの事象を引き起こす原因を特定し、特に営業店において有効な対策について検討を行う。

### 1. FAX 送受信時における発生事象

FAX 送受信時における発生事象を、送信先相違や送信情報相違による情報漏えい以外の事象についても含めて整理する。

FAX の送受信における発生事象を、送信から受信までの流れと、送信する情報の観点から整理すると以下の通りとなる。

#### < 送信から受信までの流れの観点 >

##### ・「送信漏れ・送信遅延」

送信すべき情報が送信されない。もしくは送信が適時になされない。

##### ・「送信先相違」

誤った FAX 番号による送信により、本来送信されるべき相手と異なる相手に送信してしまう。

##### ・「受信漏れ・受信遅延(相手先)」

送信した情報が、受け取るべき相手先に届かない。もしくは受け取りが適時になされない。

##### ・「受信漏れ・受信遅延(当方)」

受信された情報が、当方にて受け取るべき者に届かない。もしくは受け取りが適時になされない。

#### < 送信する情報の観点 >

##### ・「送信情報相違」

本来送信すべきでない情報が、送信情報に含まれて送信してしまう。もしくは、送るべき情報が、送信情報に含まれないで送信してしまう。

### 2. 事象を引き起こす原因

「1. FAX 送受信時における発生事象」で挙げた事象の原因を整理すると以下の通りとな

る。

「送信漏れ・送信遅延」は、送信先または送信元の業務の遅延・中断を引き起こすことにつながる。市場性を有する取引や時限性のある事務に関わるものである場合には、価格変動損や損害賠償等の金銭的な損失につながり得る。

当該事象は、送信すべき情報が網羅的に把握されていない、または、送信された情報と送信されていない情報についての識別がされていないことにより生じる。繁忙日においては連続的に、複数の職員が FAX 送信を行う状況も考えられる。そのような時に、送信漏れ・送信遅延が生じ易いことに注意を要する。

「送信先相違」は、第三者に情報が漏えいする結果となり、送信した情報が個人情報を含む場合には、個人情報保護法にも違反することになる。FAX 送受信の際の事故の典型的パターンであり、最も注意を要する事象である。

当該事象は、FAX 番号を手入力により実施している場合の入力ミスや、送信先番号の聞き間違い、または登録ミスにより生じる。そのほかにも取引先の事務所移転に伴う FAX 番号の変更など、登録情報が更新されないために生じる可能性についても注意を要する。

「受信漏れ・受信遅延(相手先)」は、「送信漏れ・送信遅延」と同様に、送信先または送信元の業務の遅延・中断を引き起こすことにつながる。

当該事象は、受信者が明確に特定(FAX 受取人欄に氏名を記入)されていない場合に生じうるが、多くの場合は送信先の受信管理体制の不備に起因して生じる。取引先への営業の際には、取引先の事務処理体制についても可能な範囲で把握しておくことで、低減できるリスクである。

「受信漏れ・受信遅延(当方)」も、送信先または送信元の業務の遅延・中断を引き起こすことにつながる。

当該事象は、受信した情報が網羅的に把握されていない、または、受信された情報が適当な受取人に適時に渡されたことについて識別(確認)されていない場合に生じる。FAX 管理の担当者が明確にされていない場合に、複数の職員が受信した FAX を随時処理している場合には、仮に受信簿が整備されていたとしても、受信情報について網羅的な把握は不完全となり、受信漏れ・受信遅延が生じる可能性があることに注意を要する。

「送信情報相違」は、本来送るべきでない情報が含まれたまま送信されてしまった場合には、意図せずして情報漏えいになり得るため、「送信先相違」と共に最も注意を要する事象である。

当該事象は、送信前の送信情報の適切性の確認(承認)が不十分である場合や、送信

可能な情報についての基準が存在しない、もしくは、基準について十分な理解を有していない者が送信する場合に生じる。同姓同名や似たような名称の取引先など、誤った情報を送信しないように細心の注意が必要である。

以上をまとめると、対策を講じるべき事項は次のように整理される。

< 対策を講じるべき事項 >

- ・「送信情報の網羅的把握」
- ・「送信状況の把握」
- ・「送信番号の正確性の確保」
- ・「受信情報の受け取り状況(相手方)の把握」
- ・「受信情報の網羅的把握」
- ・「受信情報の受け取り状況(当方)の把握」
- ・「送信情報の適切性」

### 3. 防止策

対策を講じるべき事項に対する営業店で実施可能な防止策を挙げる。

「送信状況の網羅的把握」と「送信状況の把握」については、FAX の送信ログを元に送信簿と照合することで、「送信漏れ・遅延」の防止が可能と考えられる。また、送信の都度、送信先に受信されたかについて事後確認することも有効である。

「送信番号の正確性」については、事前登録が基本的な対策として挙げられるが、登録情報が誤っている(更新されていない)ことも想定されるため、送信先に事前連絡(事前送信)する等して、送信先が正しいものであるか確認することが有効である。また送信に際しては、不正防止の観点からも複数者による確認・承認手続きを経ることでより有効なものとなる。

「受信情報の受け取り状況(相手方)の把握」については、送信先への事前に送信する旨の連絡と送信後の受け取り確認が有効である。また当該手続きの失念を防止する上で、確認簿を設置することも有効な防止策となる。

「受信情報の網羅的把握」と「受信情報の受け取り状況(当方)の把握」については、FAX の受信ログを元に受信簿と照合することで、「受信漏れ・受信遅延」の防止が可能と考えられる。

また、営業店においては、取引先から、事前に予告無く FAX が届くことも考えられることから、取引先に対して FAX 送信の際には事前に連絡をしてもらうように周知しておく必要がある。

「送信情報の適切性」については、不正防止の観点からも送信者以外の者による使用目的、使用者名等についての事前確認・承認が有効であり、その前提として送信可能(不可能)な情報についての管理区分が設けられている必要がある。

#### 4. 有効な防止策とは

「3. 防止策」で挙げた対策は、送付状、授受伝票・管理簿、発送管理表等、実施済のものもあると思われるが、これらの手続き・ルールが形骸化していると、事故の発生を防止することは不可能である。

手続き・ルールの形骸化を防止するための基本は、各職員の手続遵守の自覚の醸成であり、手続からの逸脱を見逃さない、許さないことを営業店の運営方針とする必要がある。その為には、支店長席が中心となり、様々な機会を利用し手続遵守は、各職員を守ることと同義であり、手続からの逸脱が発覚した時の罰則を考慮した場合に、いかに逸脱が割に合わないかについて自覚させる必要がある。

また、一方で手続を遵守できる環境を作る配慮も必要である。

月末、月初等の繁忙日においては、事後承認(事後確認)など手続が必ずしも完全に遵守されない状況が生じている可能性もある。そのような状況においても、手続が実効性を伴って必ず守られるように、FAX 送受信についての責任者、担当者を明確に定めておき、手続の遵守を可能とする業務運営体制を構築することも有効な対策となる。

更に、営業上必要と考え、日常的に送受信している情報について、本当に FAX で送信する必要があるのか、他の方法で業務を遂行することができないかについて今一度、再点検することも有効な対策である。

営業店運営の範疇を超えるものではあるが参考までに記しておく、一部の金融機関では、すでにFAX送信のシステム化や集中化を実現している。これらの施策は、業務の効率性とリスク管理能力の向上の二つのメリットを享受できるものであり、非常に有効な施策であると思われる。

### (3) 顧客情報の持ち出し

顧客情報の持ち出しについては、「金融分野における個人情報保護に関するガイドライン」(平成16年12月6日金融庁告示第67号)の「個人データの管理区域外への持ち出しに関する上乗せ措置」(以後、「上乗せ措置」)に、管理態勢の必要要件が挙げられている。

<個人データの区域外への持ち出しに関する上乗せ措置>

個人データの管理区域外への持ち出しに関する取扱者の役割・責任  
個人データの管理区域外への持ち出しに関する取扱者の必要最小限の限定  
個人データの管理区域外への持ち出しの対象となる個人データの必要最小限の限定  
個人データの管理区域外への持ち出し時の照会および確認手続き  
個人データの管理区域外への持ち出しに関する申請及び承認手続き  
機器・記録媒体等の管理手続き  
個人データの管理区域外への持ち出し状況の記録および分析

実際多くの金融機関では、当ガイドラインに沿った形ですでに規程を定め、定期的な本部からの周知徹底もなされていると思われる。

そのような規程が存在する金融機関においても、当日中に持ち帰る情報については例外として管理簿への記載を省略することができるとしていたため、紛失した渉外かばんの中にあった顧客情報を特定できない事例が金融検査において指摘されている。

ここでは、顧客情報の持ち出しについて、当ガイドラインに沿った規定の存在を前提とした場合に、如何に実効性ある管理態勢を実現するかについて営業店運営の視点から説明する。

#### 1. 顧客情報の持ち出しの位置付け

顧客情報の持ち出しは、外部に情報を持ち出すことであり、様々なリスクに晒される危険がある。顧客情報の持ち出しは、あくまで例外的な行為であると位置付け、持ち出し可能な情報だから持ち出してよい、持ち出し禁止の情報だから持ち出してはいけないといった、管理規程に記された通り一遍の対応に徹するのではなく、そもそも顧客情報を持ち出さないで、業務の遂行ができないかについて、まず検討することが重要である。

単に、「情報を持ち出す、持ち出さない」といった二者択一で考えるのではなく、例えば、取引先に営業店に来店してもらうことや、パスワード、暗号化による電子メール送信等、他の手段により、解決することも選択肢に入れ、幅広く対応を検討するのが有効である。

#### 2. 持ち出し可能な顧客情報の棚卸

管理するためには、その管理対象が何であるかを把握する必要がある。営業店で取り扱う顧

客情報について、各種媒体への伝送(ダウンロード)、印刷等、物理的に外部に持ち出す(持ち出される)ことが可能な顧客情報が何であるかについて棚卸を行い、重要度に応じた管理区分を設定する必要がある。また、棚卸の結果、営業上、持ち出しを行う必要が無いと考えられる情報については、物理的また組織的に、持ち出しできない措置を講じる必要がある。持ち出しを許可する情報についても、印刷可能範囲を限定するなど持ち出せる情報について最小限にとどめる為の措置が必要となる。

### 3. 取扱者の限定

持ち出しに係る事故を防止する上で、顧客情報へのアクセス及び持ち出し可能な職員を、必要最小限に限定することも有効な対策となる。

顧客情報へのアクセス及び持ち出し可能な職員については、課内レベルでの異動も含め、職務内容と連動した形で適宜見直す必要がある。

単に権限上の扱いにとどまり、顧客情報が机の上に放置される等の無いように取扱者には店内においても厳重な管理を要請し、管理者はその管理状況についてモニタリングすることが重要である。

### 4. 持ち出し時の管理

顧客情報の持ち出し時の管理は、顧客情報の持ち出しから回収(破棄)までの全てのプロセスについて確認される必要がある。

事前に、何の顧客情報を、何の目的で持ち出し、いつ回収するのか等について、申請及び管理者による承認がなされる必要がある。

当然のこととして、手続きが省略あるいは事後承認される等、形骸化しないために普段から職員に周知徹底し、必要に応じて実施状況についての確認も必要である。

持ち出されている情報の認識と持ち出した情報が適切に管理、または回収されているかを確認する上で、管理簿の設置は不可欠である。当日持ち出し・当日持ち帰りの情報など、記録されずに情報が持ち出されることが無いように、全ての持ち出し情報が記載される必要がある。また当然のこととして持ち出された情報が、回収されていることについても記録される必要がある。

### 5. 職員への周知徹底

顧客情報の持ち出し管理態勢を実効あるものとする上で、最も重要な事は、担当者が定められた手順を遵守し、管理者により承認・確認手順が適切になされることである。

特に管理者による承認・確認手順が形骸化している場合には、その実効性は失われてしまう。そのような状態を回避する為には、支店長席が中心となり、担当者、管理者に対して、手順の遵守の重要性と、違反した場合の罰則について周知徹底し、手順が形骸化しないための措置を講じることが重要である。手順の遵守の重要性については、銀行や顧客にとっての重要

性だけでなく、各人自身を情報漏えいというリスクから守るためにも重要である旨の説明を行うことで当事者意識が醸成されると考える。

## 6. 規程の補完

冒頭に述べた、金融検査における指摘事例は、規程そのものの瑕疵に起因する事故であり、当該事例に係るリスクについては、営業店で業務を行っている担当者であればだれもが認識していたはずである。本部で定められた規定は、完璧なものではないという前提に立って管理を行う必要がある。

現場での実態を慎重に観察することで、規程の対象外となっている情報、規程で想定されていない事象、規程で定められた手続きについての抜け道など、手続面、技術面それぞれの観点から問題が見えてくることも多いと思われる。

営業店を運営する立場にある支店長席は、規程に記された事項さえ守っていれば良いと考えのではなく、規程制定の趣旨(目的)をしっかりと理解したうえで、営業店で起きている状況に即した実効性ある管理を実現するために必要な施策を打つことが重要である。