SAS ユーザー総会

金融犯罪対応業務におけるSASの活用

早川 武志
ビジネス開発本部 RIグループ マネージャ
SAS Institute Japan 株式会社

目次

金融機関の挑戦
多様化する金融犯罪

マネーロンダリングやテロ資金供与に加え、振り込め詐欺・還付金詐欺と言った不正口座利用、インターネット取引の増大に伴うなりすましやID盗難、インサイダー取引・横領等の内部不正など、金融機関は多くのリスクに晒されています。

マネーロンダリング
米国内の犯罪グループが架空の投資話などで詐取した金を埼玉、千葉などの金融機関を通じてマネーロンダリングした疑い（2007/9 共同ニュース）

詐欺
振込詐欺で264万円被害
（2009/8 産経新聞）
架空請求詐欺で約1000万円被害
（2009/8 読売新聞）

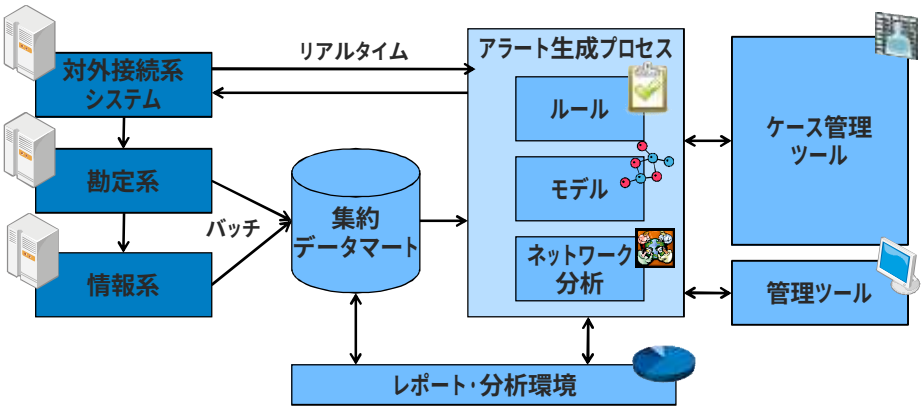
金融機関

横領
顧客の預金など総額で計約1億5800万円を着服（2008/8 産経新聞）

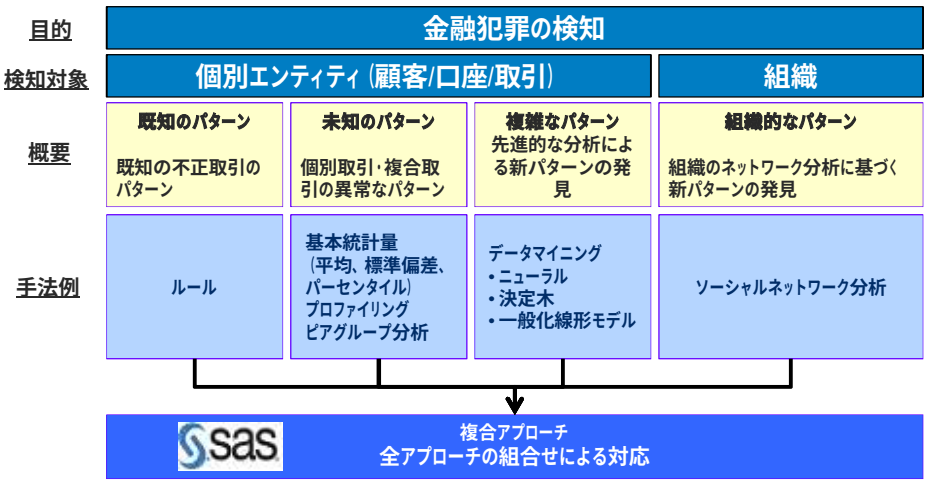
インサイダー取引
融資担当が企業のM＆A（合併・買収）に関する未公開情報をもとに
株のインサイダー取引を行っていた疑い（2009/6 産経新聞）
公開買い付け（TOB）した際、元社員は公表前に情報を把握し、知人に同社株の購入を促したり、自ら買い付け（2009/8 日経）

SASの挑戦
金融犯罪の徴候を発見するシステムへの応用

金融犯罪の徴候を発見するためのシステム機能として、①金融機関が持っているシステムのデータを集約②バッチプロセスにより金融犯罪の徴候とされる「アラート」を生成
③アラートを詳細調査することで、本当の金融犯罪を識別していく（ケース管理）
④統合的なレポート・分析環境⑤システム管理が挙げられます。



アラート検知のためのHybrid (複合) アプローチ



アラート検知のためのHybrid(複合)アプローチ

ルール (既知のパターン)

ルールの例

IF **商品** = xxx and **総入金額** > **しきい値**
Then ;
アラート生成
Else ...;
「入金額超過」ルール

IF **送金先** = **イラン**
Then ;
アラート生成
Else ...;
「制裁対象地域への送金」ルール

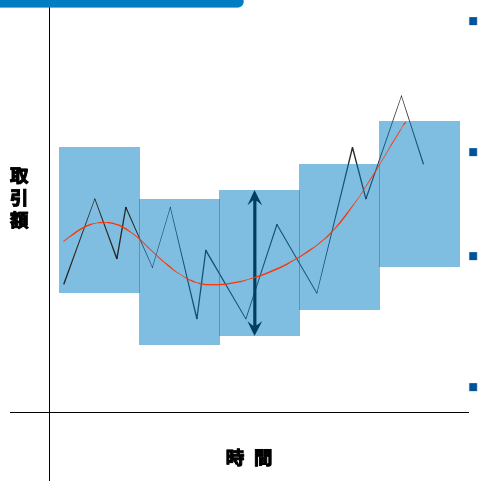
IF **月間海外送金額/月間送金額** > **しきい値**
Then ;
アラート生成
Else ...;
「海外送金比率高」ルール

- 属性や、取引振りの集計をもとに、設定された閾値を超過 (もしくは下回る) ケースをアラートとして抽出する。
- プログラム的には条件分岐であらわされるため、条件を決めさえすれば実装は比較的簡単
- 閾値は外部ファイルやDBからパラメータとして渡される方が運用しやすい
- 条件を緩く設定すれば大量に、厳しく設定すればアラートが発生しないため、十分なデータ分析が必要。

アラート検知のためのHybrid(複合)アプローチ

プロファイリング（未知のパターン）

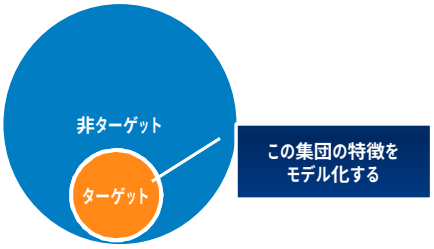
プロファイリングのイメージ

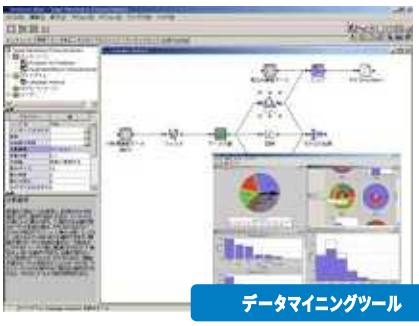


- ある個人の取引を時系列にならべ、一定範囲の取引額の偏差を取り、その偏差より「一般的な範囲」を決定する。
- ある取引が、この期間内で設定された「一般的な範囲」を超過した場合にアラートを生成する。
- 個人の取引動向をベースに異常となる領域が決定されるので、絶対的な閾値より個々のデータの状況が反映されやすい。
- 一般的な範囲の決定には「標準偏差×2」（2シグマ）が用いられることがあるが、十分なデータ分析による検証が必要

アラート検知のためのHybrid(複合)アプローチ

データマイニング（複雑なパターン）



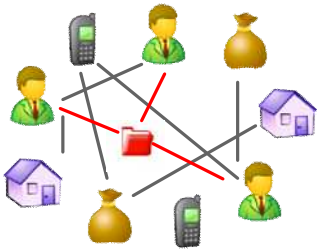


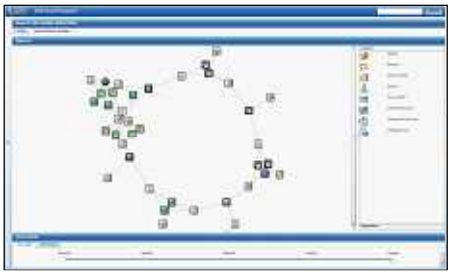
データマイニングツール

- すでに既知のマネーロンダラー、もしくはテロリストがいる前提で、ターゲット集団の傾向をデータマイニング手法を使ってモデル化する
- 手法は決定木、ロジスティック回帰、ニューラルネットワークなどが利用できると考えられる。
- できたモデルは定期的に運用し、顧客のマネーロンダリングリスクを計算して一定値以上であればアラートを生成することが想定される。
- 日本では、「疑わしい取引の届出」まではできるが本当にターゲットだったかという情報を正確に入手することは現時点では困難。

アラート検知のためのHybrid(複合)アプローチ

ソーシャルネットワーク分析 (組織的なパターン)





- 属性や、取引の相手先などをリンクしていくことにより、ネットワークを形成して、ネットワークの情報からターゲット集団を発見する手法
- ネットワークの作成方法は2種類
  - ハードリンク (属性が一致)
  - ソフトリンク (行動によりリンクが形成)
- ネットワークの接続数や集団の相互関係から指標を計算し、しきい値以上の集団をアラートとして抽出する
- 単一のエンティティでは判別し難いケースにおいて有効と考えられる。

9

まとめ

- 金融機関において、各種金融犯罪対策の必要性が高くなっている
- 金融犯罪対策システムの機能は一般的に下記となる
  - データを集積して
  - 疑わしい取引を見つけ出し
  - 詳細調査する
- 検知のアプローチは以下4パターンがあるが、データマイニングとソーシャルネットワーク分析はこれからの分野
  - ルール
  - プロファイリング
  - データマイニング
  - ソーシャルネットワーク

10