Deloitte.

Deloitte Analytics

統計的異常検出の概観　前編

1. 本稿の概要： 統計的な異常検出について

【1.1 概要】

本稿では、統計的異常検出について簡単に紹介する。アナリティクスの有用な応用先である異常検出について、特徴・応用例・手法を知ってもらうことが目的である。

【1.2 異常検出とは】

異常検出とは、データの中から通常とは異なるもの(異常)を見つける(検出する)ことである。多くの場合、何らかの“好ましくないもの”を見つけることを目的として実行される。例えば、クレジットカードの使用履歴データに対して、「日本で買い物をした二時間後にブラジルで買い物をしている」等といった不審な履歴を見つけて、不正利用による被害を最小限に抑えることを目的として、異常検出は実行される。

【1.3 統計的な異常検出とは】

統計的な異常検出とは、数学的・統計的な手法を用いて自動的に異常検出を実行することである。統計的異常検出手法の例として、データの確率分布を推定する方法が挙げられる。この方法ではデータの確率分布を推定し、得られた確率分布を基にデータが異常かどうかを判断する。上記のクレジットカードの使用履歴データからの異常検出の例で言うと、カードの使用パターンの確率分布を推定し、通常の典型的なパターンから外れた珍しい使用例を異常として検出することになる。

2. 統計的な異常検出の特徴と応用

【2.1 統計的な異常検出の特徴(メリットとデメリット)】

異常検出を実行する際に統計的な手法が必要とされるのは、専門家の目視によるチェックやシナリオ分析等といった 人手による分析 と比較して有利な点があることによる。以下では、人手による分析との比較を通して統計的な異常検出の特徴について説明する。

統計的手法の利点の一つとして、大量のデータを自動的且つ高速に処理できることが挙げられる。大量のデータを人手で分析する際にはコストと時間が問題になる。統計的手法を用いて自動的に異常検出を実行することで分析に必要な人的なコストと時間を抑制できる。また、異常検出は“好ましくないもの”を早期に検出することにより、被害を最小限に抑えるという目的で使われることが多い。この為、長期間に亘る分析というのも現実的ではない場合が多い。例えば、通信ネットワークで観測される通信量に対する異常検出によって新種のウィルスの発生を見つけたいとする。この場合に、「エキスパートによる分析で100%の精度でウィルスを発見できるが、結果がでるのは一年後」というのでは被害をほとんど抑制できないという点で、異常検出の意味がほぼなくなってしまう。

統計的手法のもう一つの利点は、複雑なデータを扱えることである。多くの変数(データの項目)が観測され、それらが互いに相関している場合、そこに含まれる異常を人が直感的に把握することは難しい。一方、統計的手法は一般的に多変量(複数の変数)を入力とするように定式化されており、多くの変数からなるデータに対する分析(異常検出)を得意としている。多くの変数が互いに相関しているシステムからの異常検出の例として、通信ネットワークの異常検出が挙げられる。ネットワークを構成する通信サーバー毎の通信量(上記の「変数」に該当)が観測されていて、それらの値からネットワーク全体が異常かどうかを判定する。通信サーバー同士が連動して動作するのに対応して、通信量の間には強い相関がある。通信ネットワークの異常を検出するには、これらをまとめて分析することが必要となる。

トーマツ.

統計的手法の特徴として、人とは異なる視点から結果が導かれることが挙げられる。数学的な定式化から出発して異常検出手法を構築する為、結果に至るまでの思考方法(異常の判定方法)が人とは異なる。この特徴は統計的手法の利点にも欠点にも結び付いている。

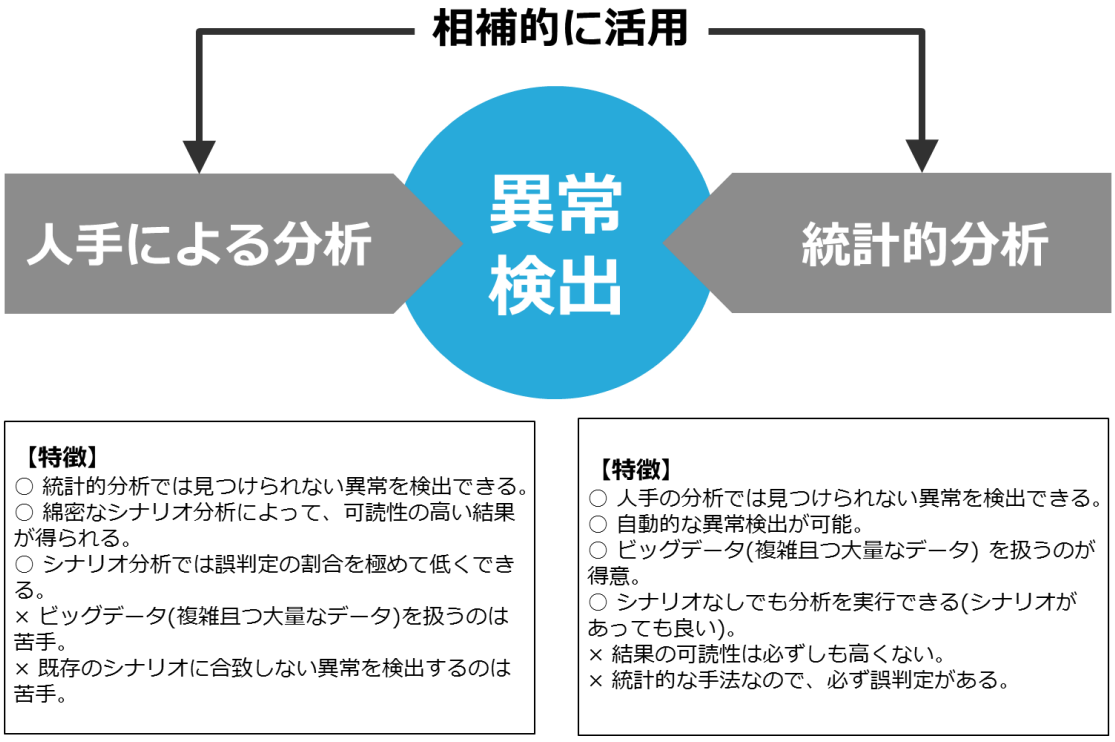
人とは異なる視点から結果が導かれることによる欠点の一つとして、精度が100%にはならないことが挙げられる。飽くまで「統計的な」手法であるから、100%の精度での異常検出は不可能であり、どうしても異常を正常と誤判定する取り逃しが発生する。従って、医療などの取り逃しが許されない分野に統計的手法「のみ」を適用してはいけない。ただし、このような分野でも統計的手法の結果を人の判断の補助として用いることはできる。

人とは異なる視点から結果が導かれることによる利点もある。それは上記の欠点とは逆に人が見逃すものを検出できることである。数学的なアプローチによって異常かどうかを判定するので、人が言語化しにくいような異常も検出できる。例えば、Webサイトの通信ログに対する異常検出によって、サイトへの攻撃を検知する場合を考える。人手による分析によって、既知の攻撃手法と類似の攻撃を精度よく検出できるが新規の手法による攻撃を即座に見つけることは難しい。一方で、統計的手法を用いて、それまでの接続パターンから外れたものを検出することで、新規の手法による攻撃を検出できる。

ここまでで述べたことは、「統計的異常検出手法とは、ビッグデータから深い洞察を得る為の方法論であるアナリティクスの一つである」とも言い換えられる。近年、複数の要素が互いに相関しあって動作するシステムから、様々な観測値を大量に取得することができるようになった。この状態や観測結果はビッグデータと呼ばれ、それらから洞察を得る為の方法論としてアナリティクスが存在する。統計的な異常検出は、アナリティクスの中の一つの手法であると言える。

ここまでで述べた通り、人手による異常検出と統計的異常検出は互いに一長一短があり、どちらか片方のみを用いるのが良いということはない。両者を相補的に用いるのが望ましい使い方である。異常検出の応用では、取り逃しが少ない方がよい場合が多い。なぜならば、不正や故障による被害を抑制するという観点では、誤警報(正常を異常と誤判定)が多少増えても取り逃し(異常を正常と誤判定)が減る方が望ましいからである。この場合、人手による分析と統計的異常検出の両者を併用して取り逃しを減らすのが良い方法だと言える。

図1. 統計的分析とシナリオ分析の統合的活用



【2.2 統計的異常検出の適用対象と応用例】

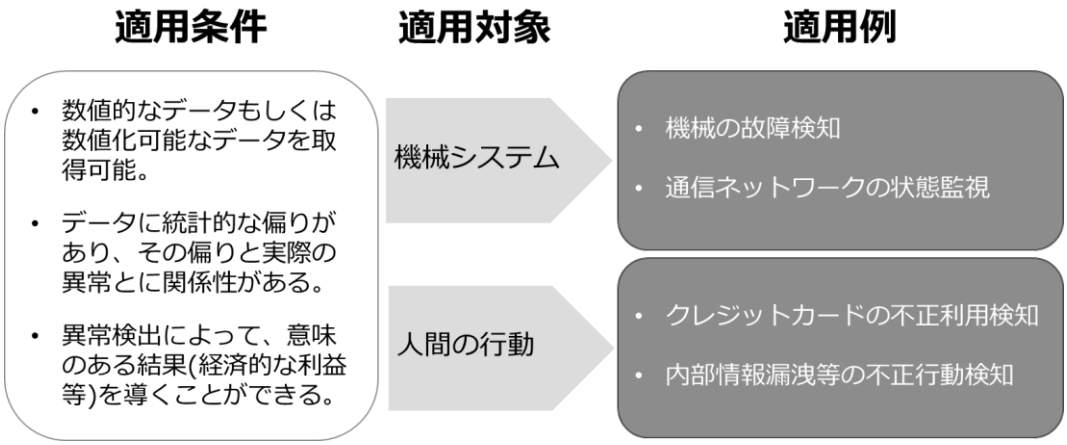
統計的な異常検出の適用対象は多岐に亘る。極端に言えば、以下の三つの条件が満たされれば統計的異常検出の適用対象となる。第一の条件は、数値的なデータもしくは加工することで数値化できるデータが収集可能であることである。統計的な分析である以上、何らかの数値が得られないことには実行自体が不可能となる。第二の条件は、異常検出によって意味のある結果が得られることである。不正や故障を見つけても得られる利益や抑制される被害が小さいのでは意味が無い。第三の条件は、取得できるデータに統計的な偏りがあり、データ中の値の偏りと異常の発生との間に関係があることである。データからは分からないことやデータ自体を取得できないものは統計的異常検出の適用範囲外であり、人手で異常を検出するしかない。

以下では、統計的異常検出の適用例を挙げ、適用対象と異常検出の目的について説明する。

統計的な異常検出は、機械的なシステムの状態監視に応用できる。例えば、機械の故障検知への応用である。機械の中のセンサーから得られるデータ(電流・電圧・温度等)を入力として異常を検出する。ここでは、検出すべき異常とは故障の発生のことである。例えば、平常時のセンサーデータの挙動をパターン化しておき、パターンから大きく外れたデータが現れたら異常とみなす。機械の場合、どこかが故障していても人の目で見える表面的な部分にはその兆候が現れないこともある。この為、人手のみでの故障検知が難しい場合もあり、統計的異常検出が必要とされる。他の例として、通信ネットワークの状態監視への応用が挙げられる。通信ネットワークから取得できる情報(主に通信量)を入力として異常を検出するものである。ここで言う異常には、通信サーバーの故障、異常な通信の発生、通信経路の異常、等の幾つかの意味が含まれる。

統計的な異常検出は、人間の行動に対する分析にも応用できる。例えば、クレジットカードの不正利用検知が挙げられる。クレジットカードの使用履歴を入力として、異常を検出する。検出された異常を不正使用の候補と見なし、契約者へ通知したりカードの使用を停止させたりする。早期に不正を検知することで、不正利用による被害を抑制できる。他の例として、不正行動検出が挙げられる。PC操作ログを入力として異常を検出する。ここで検出したい異常は、内部情報の持ち出し等の不正な行動である。例えば、個別のユーザーの操作パターンもしくは全ユーザーに共通する操作パターンから大きく外れたパターンを不正な行動の候補として抽出する。多くの場合、PCの操作ログは件数が多く、人手での分析に時間がかかる。この為、早期の検出が可能な統計的異常検出が必要とされる。

図2. 統計的異常検出の適用対象



幾つかの例を挙げたが、ここまでで列挙したのは応用例のほんの一部である、これら以外にも様々な適用例が存在する。

ここまで、統計的な異常検出について、その特徴と応用例を述べた。次回、第二回では統計的な異常検出を実現する為の手法について説明する。異常検出に適用できる統計的・数学的な手法とはどのようなものかについて、機械学習の視点から概要を解説するつもりである。

Deloitte Analytics　広瀬 俊亮

(注)当該記事は執筆者の私見であり、トーマツグループの公式見解ではありません。

お問い合わせ先
有限責任監査法人 トーマツ　デロイト アナリティクス
〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル
Tel: 03-6213-1112
e-mail: tohmatsu.analytics@tohmatsu.co.jp　URL：http://www.tohmatsu.com/jp/da