はじめに

リアルワールド（現実世界），サイバーワールド（Web 上の世界）の両方にわたって情報が大量に溢れ，これを何とか活用しなければならない，といったニーズが拡大している．データマイニングとは，大量なデータを掘り起こし，有用な知識を発見するための技術である．つまり，まさに上述のニーズに真っ向から対応する技術である．

ところで，「有用な知識」とは何であろうか？　大量のデータを処理して何を見せてくれたら我々は嬉しいのであろうか？

筆者はデータに埋もれる「有用な知識」は大きく 2 つあると考える．1 つはデータのもつ規則性であり，もう 1 つはデータに潜む異常である．特に後者――「異常」――を発見することの産業上のインパクトは極めて高い．なぜなら，それは様々なリスクの回避につながるからである．詐欺のリスク，不正のリスク，侵入のリスク，障害のリスク，故障のリスク，など様々なリスクはデータの上での異常を伴う．このようなリスクを早期に検出し，原因を追求することの意義は計り知れない．

筆者は，企業にて 20 年以上研究開発に携わってきた．企業では研究テーマを設定する際に「何にどう役に立つのか？」「どのような事業に結びつくのか？」を徹底的に検討させられる．筆者が企業の中でデータマイニングの研究を立ち上げたときも，単に，大量データから知識を発見できます，では当然通用しな

い．しかしながら，その中にあって，異常検知については広い範囲にわたってビジネスに貢献できる確かな感触をもっていた．実際に，システム運用，セキュリティ，マーケティング，製造などの数多くの現場で，異常検知が価値を生み出すチャンスが無限に広がっていたのである．こうした動機から，この分野の研究開発を 10 年以上も手がけることになった．自分なりに異常検知の学問体系を作りたい，これを基にしたビジネスを創出したい，という思いで続けてきたのである．そして「異常検知がビジネスの価値を生み出す」といった手応えは今では一層強くなっている．

本書は，筆者が上述のようなモチベーションで取り組んできた異常検出の分野について，1 つの方法論を提示するものである．本書には以下の特徴をもたせた．

1. 異常検出を行うための根本的かつ原理的な点を，できるだけ数理的に記述し，統一的な視点が得られるようにした．それは，「情報論的学習理論」と呼ばれる，情報理論・統計学に基づく機械学習へのアプローチからの視点である．反面，プラクティカルな方法を詳細に記述したり，網羅的かつ総花的にこの分野の技術方法を列挙することは避けた．むしろ，芯の通った，異常検知に取り組む 1 つの姿勢が本書によって伝わるといってよい．
2. 本書の理論に基づいて，企業の現場で数々の実証に取り組んだ成果も，差し支えない範囲でできるだけ多く紹介した．まさにデータマイニングの 1 つの理論体系が現実に「生きている」実態を豊富な事例の下に示した．

異常検知は，産業上の広い応用性があるだけでなく，それ自体，学問的にも深さと広がりをもっている．そもそも「異常とは何か？」「それをいかにして数理的にモデル化するか？」「それをいかに現場で役に立てるか？」を考えるところに，醍醐味が満ち溢れているのである．本書は，そういった部分の面白さを惜しみなく記した．そもそも本書の意図は「深い理論（数理工学的基礎）が現実に役に立つ」ことを伝えることにある．

本書を読み進める上での事前知識としては，確率論や統計学の基礎的知識を仮定している．データマイニングの基礎は機械学習であり，機械学習の基礎は統計理論であるからである．機械学習に関しても，初等的な知識があればなお

良い．実際，本書の中では機械学習の中でも先端の理論を駆使している．ただし，理論の核となる部分に関しては，別途紙面を割いて，その数学的基礎だけを概説しているので，機械学習に関しては予備知識がなくてもかまわない．むしろ，「異常検知」という分野への知的好奇心があれば，読み切れると信じている．

また，本書は，異常検知の方法と実際を記しているが，ここにかいてある方法論をそのまま実装するつもりで読んではいけない．実装や実適用には多大なノウハウやチューニングが必要であり，そのような記述は煩雑になるため本書では省略しているからである．むしろ，異常検知に対する基礎的な方法論や哲学をを吸収するつもりで読んでいただきたい．そして，そこに関わる多くの数理的基礎技術の 1 つ 1 つが，異常検出という問題を通じて有機的につながり，組み合わせることで，現実問題をみごとに解決できるのだ，というところを感じてほしい．数学はそれ自体がアート（芸術）であるが，現実問題を解決できる数理工学的側面もまた高度なアートであるのだから．

本書の構成

第 1 章では，本書で扱う異常検知の問題の意義を説明する．データマイニングにおける異常検知の位置づけを与えるとともに，異常検知のモチベーションをセキュリティ，障害検出・故障検出，詐欺検出といった具体的視点から与える．

第 2 章では，本書の異常検知に対する基本的考え方を示す．それは確率モデルの学習とそれに基づくデータの異常度合いのスコアリングのプロセスとして統一的に与えられる．本書では統計的モデルの分類により異常検出の問題を，**外れ値検出**，**変化点検出**，**異常行動検出**といった 3 つの基本問題に分類することを示す．続く第 3，4，5 章がその詳細の説明にあたる．

第 3 章では，第 1 の問題である**外れ値検出**を扱う．侵入検出を動機づけとして本問題を導入する．次に，従来手法として，マハラノビス距離に基づく外れ値検出を紹介し，この問題点を解決する手段として，適応的外れ値検出手法である **SmartSifter** を紹介する．SmartSifter の原理とアルゴリズムの詳細について解説した後，その侵入検出問題，不審医療データ検出問題への応用例を示

す．また，アンサンブル学習と呼ばれる手法によって異常検出の精度を増強できることを示す．さらに，異常検出の結果得られた異常データのパタンをルール形式で知識化する方法を示す．最後に，外れ値検出の分野に関するトレンドを概説する．

第 4 章では，第 2 の問題である**変化点検出**を扱う．未知ウイルスの早期検出を動機づけとして本問題を導入する．次に，従来手法として，統計的検定に基づく変化点検出を紹介し，この問題点を解決する手段として，時系列の 2 段階学習に基づく変化点検出手法である **ChangeFinder** を紹介する．ChangeFinder の原理とアルゴリズムの詳細について解説した後，その応用例として，未知攻撃の検知や東証株価指数の変化点検知を示す．最後に，変化点検出の分野のトレンドを示す．

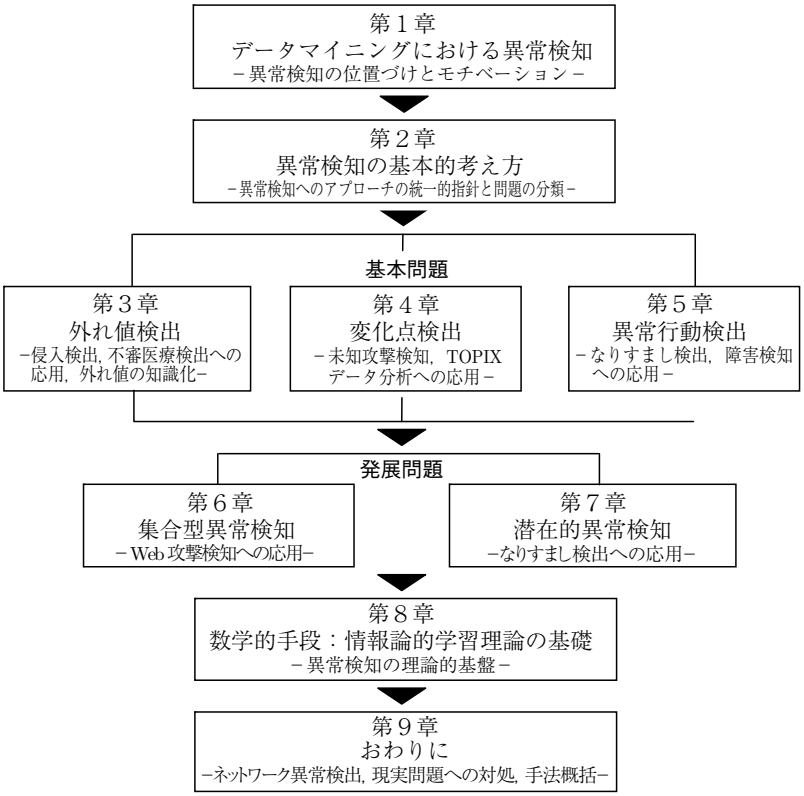
第 5 章では，第 3 の問題である**異常行動検出**を扱う．サイバー犯罪の検出を動機づけとして本問題を導入する．次に，従来手法として，ナイーブベイズ法に基づく異常行動検出を紹介し，この問題点を解決する手段として，適応的異常行動検出手法である **AccessTracer** を紹介する．AccessTracer の原理とアルゴリズムの詳細について解説した後，そのなりすまし検出や障害検出への応用例について示す．最後に，異常行動検出の分野のトレンドを示す．

第 6，7 章は第 3，4，5 章の基本問題をより拡張させた発展問題として位置づけられる．

第 6 章では，同一データに対して上述の変化点検出と異常行動検出を組み合わせて異常検出を行う方法である**集合型異常検知**を扱う．ここで，データの定量的側面を利用して変化点検出を，データの定性的性質を利用して異常行動検出を行い，そのスコアを統合する．Web 攻撃検知への応用例を示す．

第 7 章では，これまでの異常検知を顕在的異常の検知として，**潜在的異常の検知**を行う方法を扱う．これはデータの確率モデルに含まれる潜在変数のダイナミクスに対して異常検出を行うものである．なりすまし検出への応用を示す．

第 8 章では，本書の理論的基礎となる**情報論的学習理論**とその周辺について，本書に必要な数学的概念のみを取り上げ，これを詳しく説明する．その内容は，EM アルゴリズムと忘却型アルゴリズム，モデル選択，動的モデル選択，拡張型確率的コンプレキシティなどにわたる．



本書の構成

第 9 章では，今後発展する問題としてネットワーク異常検出の問題を取り上げて簡単に動向を紹介した後，現実の問題に対処するためのポイントに触れ，最後に本書の問題と解決手法を概括して締めくくる．

以上で説明した本書の構成を模式的に示したのが上図である．

謝辞

本書は，主に筆者がすでに発表した論文の内容を中心に構成されている．それらの論文の共著者との共同研究なしには本書は生まれなかった．以下の共

同研究者の方々に深く感謝いたします．竹内純一氏（当時：日本電気株式会社 (NEC)，現：九州大学），Graham Williams 氏 (CSIRO)，Peter Milne 氏（当時 CSIRO），丸山祐子氏（当時：日本電気株式会社 (NEC)，現：野村證券株式会社），広瀬俊亮氏（日本電気株式会社 (NEC)），山形昌也氏（日本電気株式会社 (NEC)），岩井博樹氏（LAC 株式会社）．

また，本書出版にあたり共立出版をご紹介いただきました杉原厚吉先生（当時：東京大学，現：明治大学）に深謝いたします．とともに，本原稿を丁寧に読んでコメントいただいた櫻井瑛一氏（東京大学）に感謝いたします．