目　　次

第 1 章 データマイニングにおける異常検知 **1**

1.1 異常検知の位置づけ 1

1.2 セキュリティ分野からの要請 3

1.3 障害検出・故障診断からの要請 5

1.4 詐欺検出からの要請 7

第 2 章 異常検知の基本的考え方 **8**

第 3 章 外れ値検出 **11**

3.1 侵入検知と外れ値検出 11

3.2 マハラノビス距離に基づく外れ値検出 13

3.3 外れ値検出エンジン SmartSifter 15

3.3.1 SmartSifter の基本原理 15

3.3.2 SDLE アルゴリズム 19

3.3.3 SDEM アルゴリズム 20

3.3.4 SDPU アルゴリズム 24

3.4 外れ値検出の応用例 27

3.4.1 ネットワーク侵入検出への応用 27

3.4.2 不審医療データの検出への応用 29
3.5 アンサンブル学習に基づく外れ値検出の強化 32
3.6 外れ値検出からセキュリティ知識の発見へ 33
3.6.1 外れ値フィルタリングルールの生成 33
3.6.2 確率的決定リストの学習 36
3.6.3 ネットワーク侵入検出への応用 41
3.7 外れ値検出の動向 44

第 4 章 変化点検出 45

4.1 未知ウイルスの早期検知と変化点検出 45
4.2 統計的検定に基づく変化点検出 46
4.3 変化点検出エンジン ChangeFinder 48
4.3.1 ChangeFinder の基本原理 48
4.3.2 SDAR アルゴリズム 51
4.4 変化点検出の応用例 54
4.4.1 攻撃検知への応用その 1：MS.Blast 54
4.4.2 攻撃検知への応用その 2：LOVGATE 55
4.4.3 階層的変化点検出に基づく DDOS 攻撃の検知 56
4.4.4 東証株価指数の変化点検出 57
4.5 変化点検出の動向 58

第 5 章 異常行動検出 59

5.1 サイバー犯罪の検出と異常行動検出 59
5.2 ナイーブベイズ法による異常行動検出 60
5.3 異常行動検出エンジン AccessTracer 62
5.3.1 AccessTracer の基本原理 62
5.3.2 行動モデリング 64
5.3.3 SDHM アルゴリズム 68
5.3.4 動的モデル選択 70
5.3.5 異常スコアリング 74

5.4　異常行動検出の応用例 79
5.4.1　なりすまし検出への応用 79
5.4.2　syslog からの障害検出への応用 1：問題設定と前処理 . 81
5.4.3　syslog からの障害検出への応用 2：障害予兆検出 83
5.4.4　syslog からの障害検出への応用 3：新障害パタンの同定 86
5.4.5　syslog からの障害検出への応用 4：障害の相関分析 . . 88
5.5　異常行動検出の動向 91

第 6 章 集合型異常検知 **93**
6.1　Web 攻撃検知と集合型異常検知 93
6.2　集合型異常検知の基本原理 94
6.3　集合型異常検知の応用例：Web 攻撃検知 97
6.4　Web 攻撃検知の動向 100

第 7 章 潜在的異常検知 **101**
7.1　潜在的異常とは？ 101
7.2　潜在的異常検知の基本原理 103
7.3　モデル変動ベクトルの解釈 108
7.4　潜在的異常検知の応用例 111
7.4.1　実験の設定 111
7.4.2　人工データへの適用 112
7.4.3　なりすまし検出への適用 114

第 8 章 数学的手段：情報論的学習理論とその周辺 **118**
8.1　EM アルゴリズムとオンライン忘却型学習アルゴリズム 118
8.2　ヘリンジャー距離の近似的計算方法 124
8.3　Burge and Shawe-Taylor のアルゴリズム 125
8.4　モデル選択と MDL 規準 127
8.4.1　MDL 規準と確率的コンプレキシティ 127
8.4.2　MDL 推定の収束速度 132
8.4.3　逐次的符号化と Minimax Regret 133

8.4.4 予測的確率的コンプレキシティ 136
8.4.5 ベイズ符号化と Mixture 形式の確率的コンプレキシティ 139
8.5 拡張型確率的コンプレキシティ 140
8.5.1 拡張型確率的コンプレキシティと一般化 MDL 140
8.5.2 一般化 MDL の収束速度 142
8.5.3 拡張型確率的コンプレキシティと Minimax Regret . . 143
8.6 動的モデル選択 146
8.7 対象化モデル変動ベクトルの分解 150

第 9 章 おわりに **155**
9.1 今後の発展：ネットワーク異常検知 155
9.2 現実の問題に向かうために 158
9.3 まとめ 159

参考文献 **161**

索 引 **169**