ディープラーニングに基づく異常検知技術 ――DeAnoS: Deep Anomaly Surveillance

渡辺 敬志郎（わたなべ けいしろう） /田尻 兼悟（たじり けんご）
中野 雄介（なかの ゆうすけ）
NTTネットワーク基盤技術研究所

本稿では，ネットワークサービスのプロアクティブな保守運用に向けてNTT研究所で検討を進めているディープラーニングに基づく異常検知技術（DeAnoS: Deep Anomaly Surveillance）の概要と事業会社における検証状況を紹介します．

背　景

NTTネットワーク基盤技術研究所では，ICTシステムの状態変化の早期検知を目的として，オートエンコーダ（AE）を活用した異常検知技術（DeAnoS: Deep Anomaly Surveillance）の開発に取り組んでいます[(1)~(3)]．本稿ではDeAnoSに関してNTT R&Dフォーラム2018（秋）で展示した内容を紹介します．

DeAnoSの概要

DeAnoSで活用しているAEは，データに内在する複雑な構造の学習を可能とするディープラーニングの一種であり，AEによる異常検知技術に注目が集まっています．AEでは中間層の次元を入出力層より少なく設定し，入力層のデータを出力層で再現するようにパラメータを学習することで，中間層においてデータの次元削減が行われます．AEを用いた異常検知では，正常なデータは入力データ空間上において，低次元表現が可能なある多様体の周辺に分布するという前提に基づいています．具体的には，学習時には，システムが正常に動作している期間に観測した各種データによって「正常な状態」を学習し，テスト（異常検知）時には，現時点のデータが上記のように学習されたAEに入力され，入出力層のベクトル間の距離を異常度として出力します（**図1**）．異常度がしきい値を超えると異常として検知します．

なお，入力するネットワークデータとしては，SNMP（Simple Network Management Protocol）/MIB（Management Information Base）に基づくリソース・トラフィック情報やNetflowに基づくフローデータといった数値データに加え，テキスト情報であるルータやサーバのsyslogも対象としています．syslogは，syslog分析技術[(4)]を用いてID化し，各IDの出現回数を用いてテキストデータから数値データに変換します．こうすることで，syslogも含めた学習を可能としています．

さらに，異常を検知するだけでなく，異常検知時にその要因を推定するための検討も進めています[(5)]．具体的には，AEによって異常が検知されたら，どの入力次元が原因で異常度が高くなったかをスパース最適化によって推定する技術を検討しています．この技術では，異常度に対する各入力次元の寄与度を算出しており，これにより異常検知後の切り分け作業の効率化が期待できます．

事業会社におけるDeAnoSの検証状況

現在，事業会社の協力の下で，実際

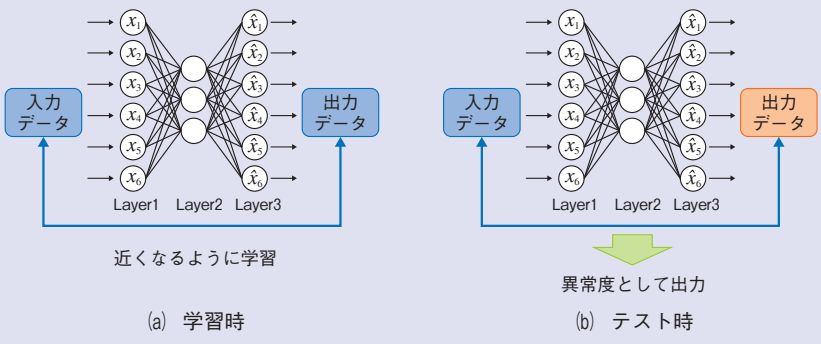


図1　AEの仕組み

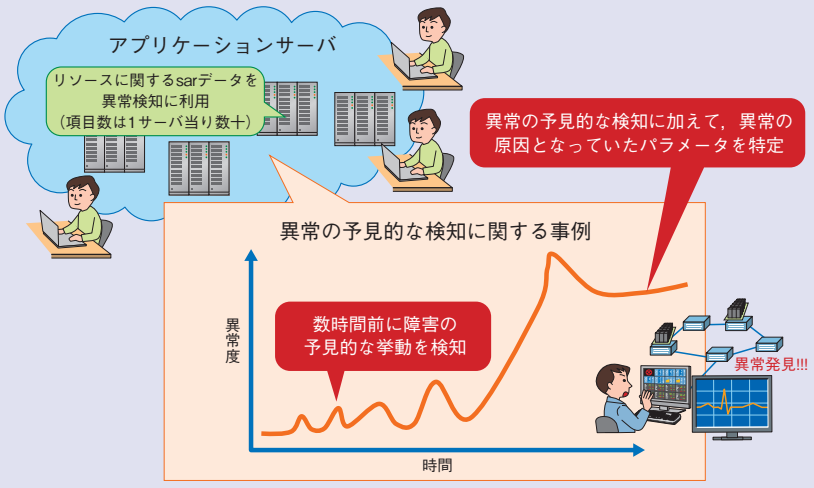


図２　NTT東日本との取り組み

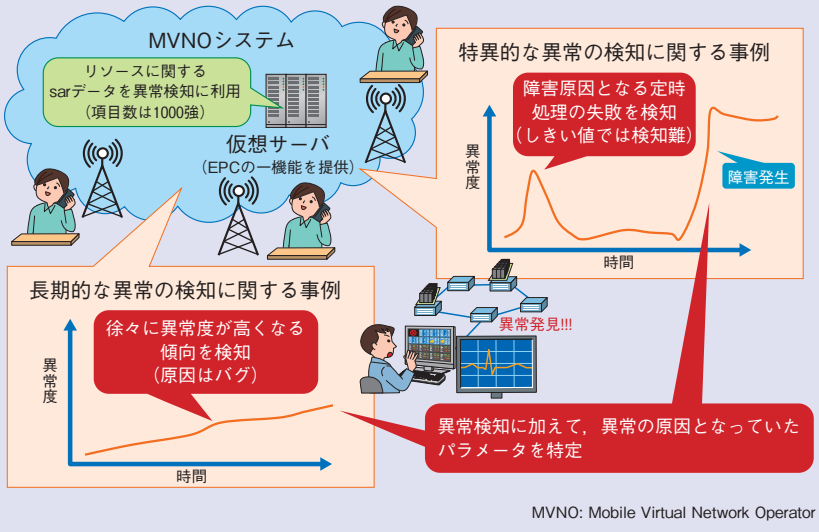


図３　NTTコミュニケーションズとの取り組み

のサービスから取得した運用データに基づきDeAnoSの検証を進めており，技術の有効性検証や実用に向けた課題の抽出を行っています．本稿ではNTT東日本とNTTコミュニケーションズとの取り組みについて紹介します．まずNTT東日本 高度化推進部との取り組みでは，アプリケーションサーバ群における異常の予見的・早期検知とその原因となっていたパラメータの推定を行いDeAnoS の有効性を確認しました（**図２**）．また，NTTコミュニケーションズ ネットワークサービス部との取り組みにおいては，特異事象や長期的な傾向の変化を対象として分析を行い，異常検知に加えてその原因となるパラメータの推定が可能である事例を確認しました（**図３**）．

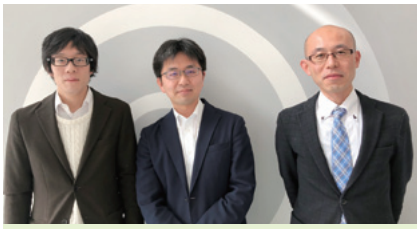
今後の展開

本稿では，NTTネットワーク基盤技術研究所が検討しているDeAnoSの概要を示すとともに，ネットワーク異常検知技術に関する事業会社との検証状況について紹介しました．

今後は事業会社との技術検証を進めてブラッシュアップを継続的に行うとともに，実フィールドで技術を利用するための環境を整備します．また，ネットワーク異常検知技術の課題として，異常検知した際の要因の解釈性改善や多様な環境への適応などが挙げられ，これらを解決するための研究開発を継続して行います．

■参考文献

(1) 中野・池田・渡辺・石橋・川原：“オートエンコーダによるネットワーク異常検知，” 2017信学総大，B-7-33，2017.
(2) 池田・中野・渡辺・石橋・川原：“オートエンコーダを用いたネットワーク異常検知における精度向上に向けた一検討，” 2017信学総大，B-7-34，2017.
(3) 川原：“ネットワークオペレーション・制御技術の高度化に向けたAI/機械学習の活用について，” 2017信学ソ大，BT-2-1，2017.
(4) T. Kimura, A. Watanabe, T. Toyono, and K. Ishibashi: “Proactive Failure Detection Learning Generation Patterns of Large-scale Network Logs，” IEEE/IFIP CNSM 2015 (mini-conf.)，Barcelona，Spain，Nov. 2015.
(5) 池田・石橋・中野・渡辺・川原：“オートエンコーダを用いた異常検知におけるスパース最適化を用いた要因推定手法，” 信学技報，Vol.117，No.89，pp.61-66，2017.



（左から）田尻　兼悟/ 渡辺　敬志郎/ 中野　雄介

NTT研究所では，Network-AIに基づく保守運用の効率化・高度化に関する技術の提案を通じて，より良いサービス提供環境の整備に貢献していきたいと考えています．

◆問い合わせ先
NTTネットワーク基盤技術研究所
通信トラヒック品質プロジェクト
TEL　0422-59-4349
FAX　0422-59-6364
E-mail　dnn-ad-ext-ml@hco.ntt.co.jp