JNSA 2025年度活動報告会

サイバーセキュリティにおけるAI活用の今

株式会社ChillStack　伊東 道明

自己紹介

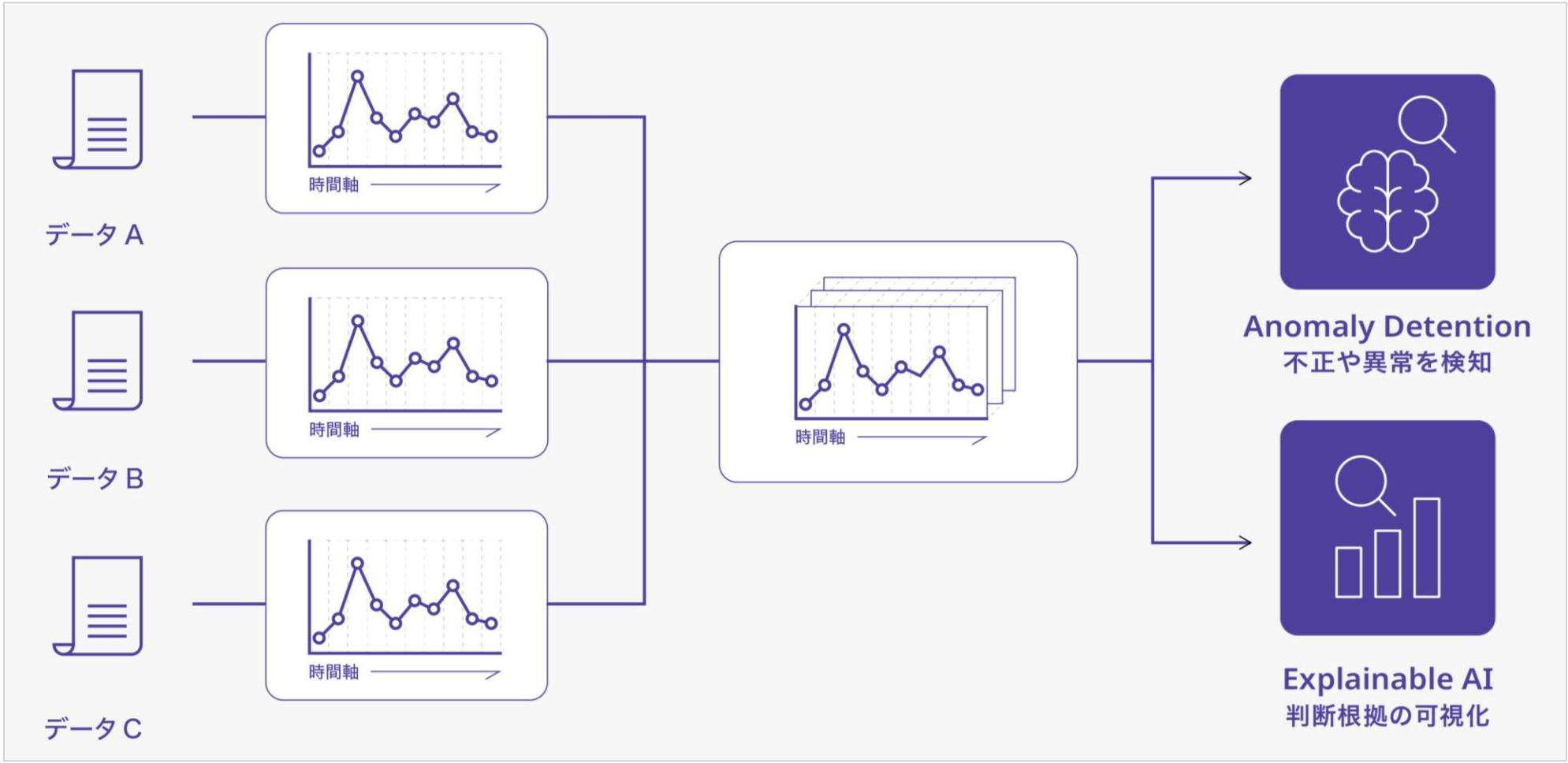
株式会社ChillStack　代表取締役CEO

伊東 道明

2015年よりAI×セキュリティ領域の研究に従事。
国際学会IEEE CSPA2018にて最優秀論文賞、IPAセキュリティキャンプ・アワード2018 最優秀賞を受賞。
自身が国際セキュリティコンテストでの優勝経験をもち、
IPA セキュリティキャンプにて人材育成に貢献。
2018年にChillStackを創業。
Forbes 30 U30 Asia 2025 AI部門　選出。

ChillStackで取り組んでいる内容

多次元 / 時系列のデータをインプットして、異常を検知するサービスを提供しています。
異常検知モデルは、データや解決したいタスクに合わせて特化型AIを個別に開発しています。



統計 + 特化AI + 生成AI の3段構えで活用

近年用いられている“AI”というワードには、幅広い技術が内包されていて、それぞれ得意なことが異なってきます。

例）

- 古典的な統計技術の活用 → 人が理解しやすい可視化など
- 解決したいタスクに特化した機械学習技術の活用 → 安定した検知や速度の実現など
- 汎用的な生成AI → 複雑な業務の支援など

やりたいことに適したAI技術を活用していくことで、安定した速度・精度の実現や安心感の醸成、複雑な作業の効率化などを目指しています。

直近の動向：AIの利活用領域が拡大

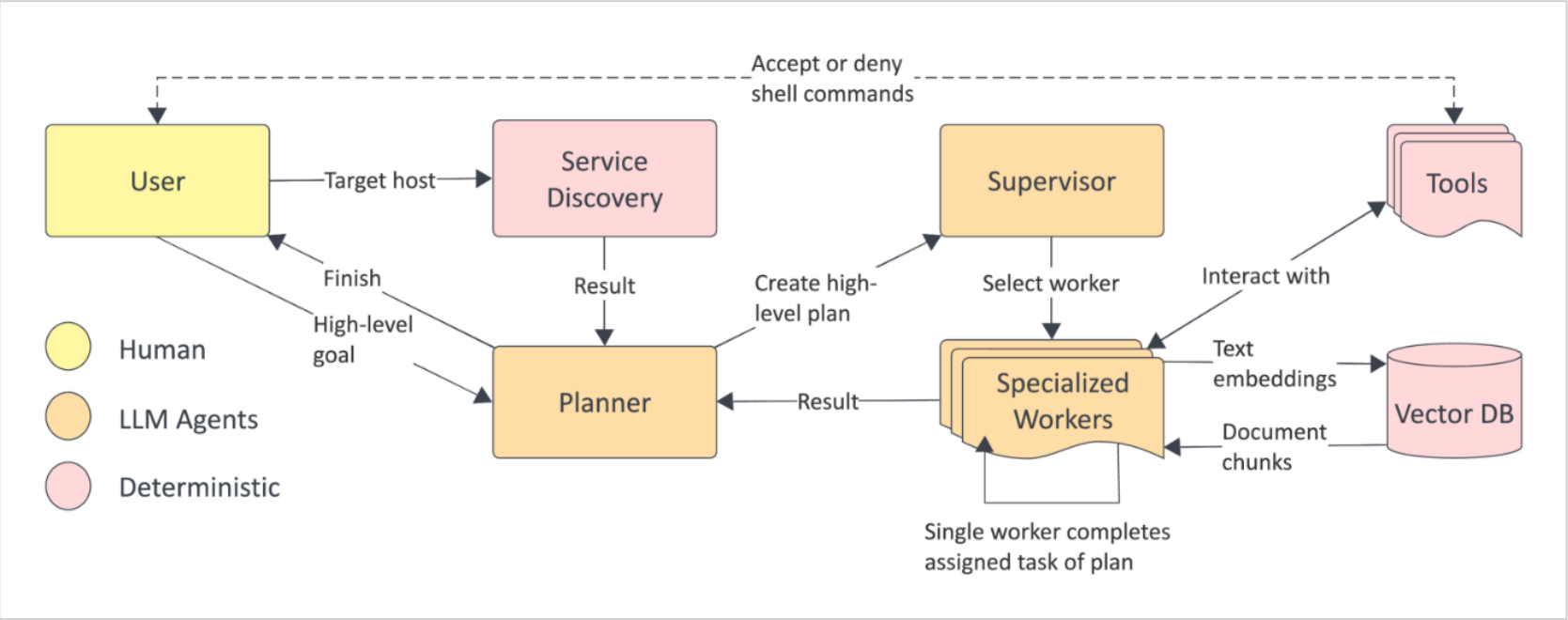
当社が取り組んでいる領域はいわゆる Blue Teaming と呼ばれるようなものに近いですが、直近では実務レベルでのRed Teaming 領域への活用も進んできていると感じています。

その辺りも含め、本日は幅広くディスカッションできればと思います。

例）

AutoPentest: Enhancing Vulnerability Management With Autonomous LLM Agents

GPT-4oとLangChainを組み合わせることで、タスクを自動管理しながらペネトレーションテストを実施できる手法を提案。



https://arxiv.org/abs/2505.10321