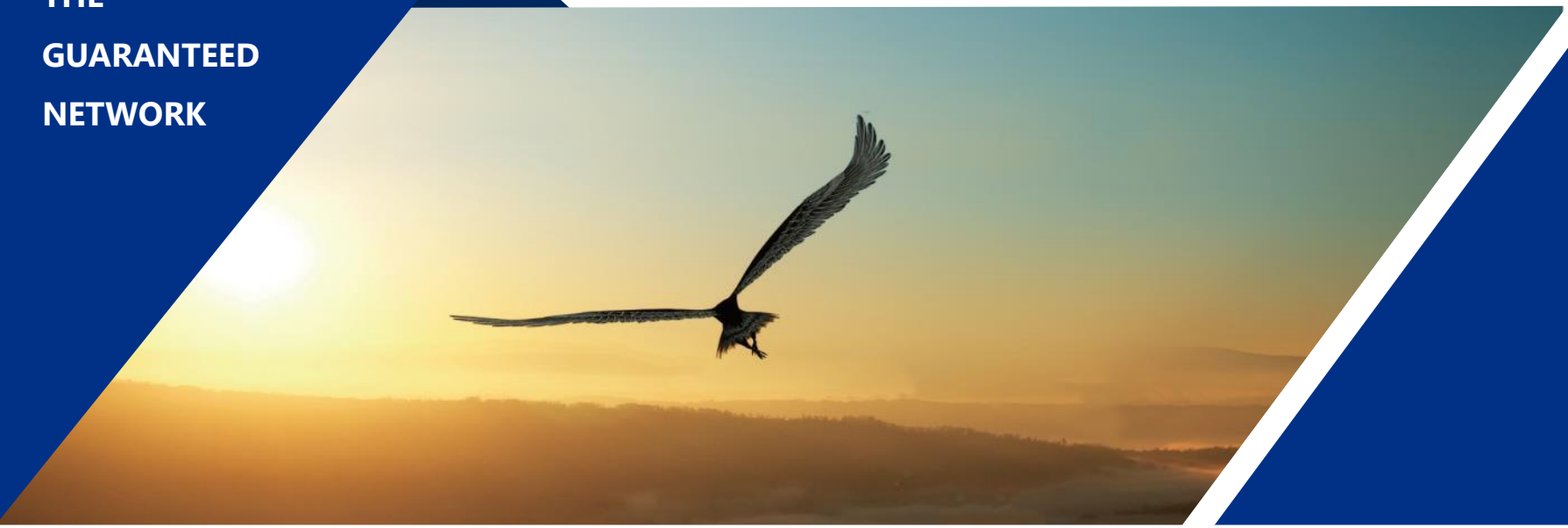
The Guaranteed Network
いちばん近くで、もっと先へ。

C9 Flow技術まとめ
～基礎から最新動向・応用まで～
最新のFlow技術をキャッチアップ

THE
GUARANTEED
NETWORK



ALAXALA
A FORTINET Company

2023/11/21

自己紹介

◆名前

- Hiroki Yano

◆所属

- ALAXALA Networks Corp.
  - ✓Director, Solution Development Department

アジェンダ

- はじめに
- サイレント障害とは？
- 機械学習を使ってサイレント障害を検知
- 機械学習の応用例
- 導入・運用するためのステップ

はじめに

このセッションでは、Flow技術を使って取得した情報と機械学習を組み合わせることで可能になる、いくつかのユースケースの紹介をしたいと思います。

まずユースケースの一つとして、サイレント障害に対する対策としての利用例を紹介します。

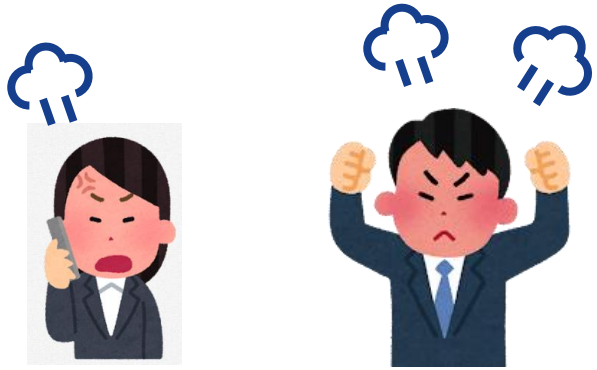
次にそれ以外のユースケースや導入に関するステップなどを簡単に紹介します。

サイレント障害とは？

ユーザ通信に影響がでているにもかかわらず、アラート(警報)が出ない障害
ユーザからのクレームなどで発覚するケースが多い
アラートが上がらないため、原因調査のとっかかりが無く、長期化・重大障害になる

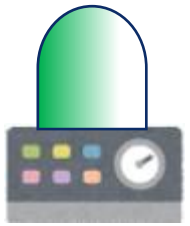
ユーザ側

インターネットがつながらない
通信が遅い
動画や会議の音声や映像が乱れる



ユーザ
クレーム

運用者



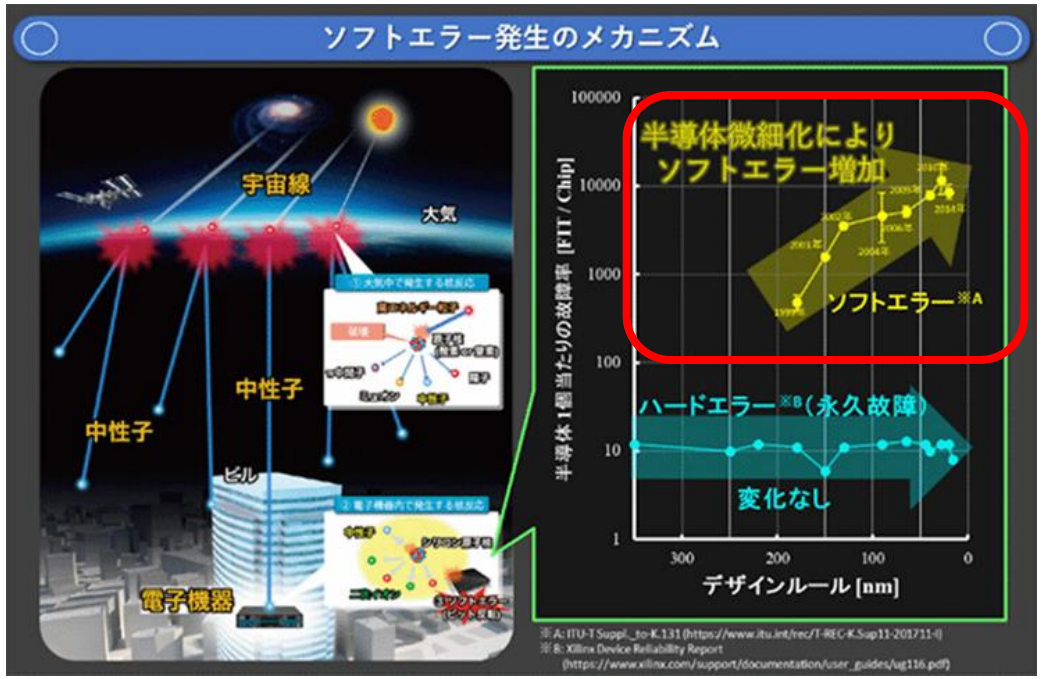
アラートはあがっていない。

原因がわからない！

通信設備におけるサイレント障害の要因

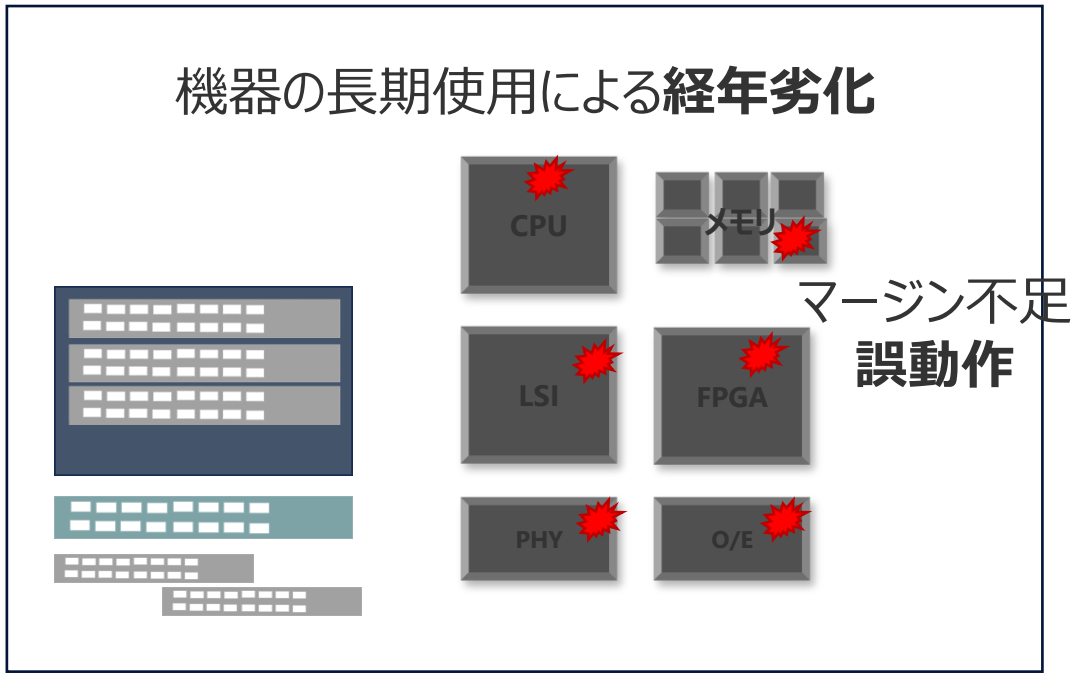
通信設備のソフトエラーや経年劣化等により、サイレント障害が多発する傾向
ソフトエラーとは、宇宙線により発生した中性子により電子機器が誤動作する事象

① ソフトエラーに起因するサイレント障害



ソフトエラー発生のメカニズムを表したイメージ
(出典：https://group.ntt/jp/newsrelease/2020/11/25/201125a.html)

② 経年劣化やマージン不足に起因するサイレント障害

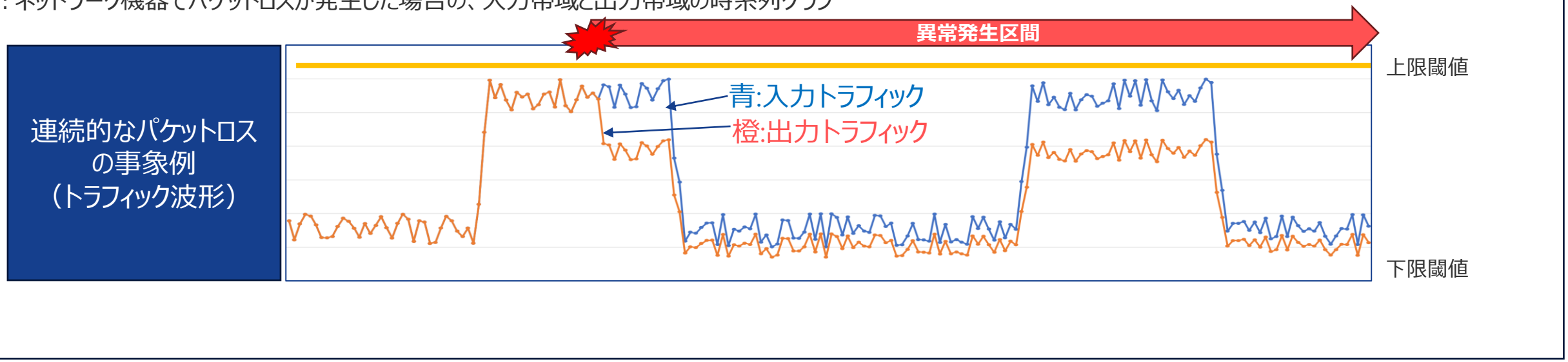


- **2021年にNTTが発表した情報では、ソフトエラーの影響は、年間3万~4万件発生している。**
- **大部分は、自動検知・自動修復されるが、未検知の可能性もある。**
- **未検知となった障害は、サイレント障害となるため、大規模障害となるリスクをはらんでいる。**

機械学習を使って、サイレント故障を検知

ソフトエラーや経年劣化による誤動作　→　『連続的なパケットロスの事象』 につながることが多い

図：ネットワーク機器でパケットロスが発生した場合の、入力帯域と出力帯域の時系列グラフ

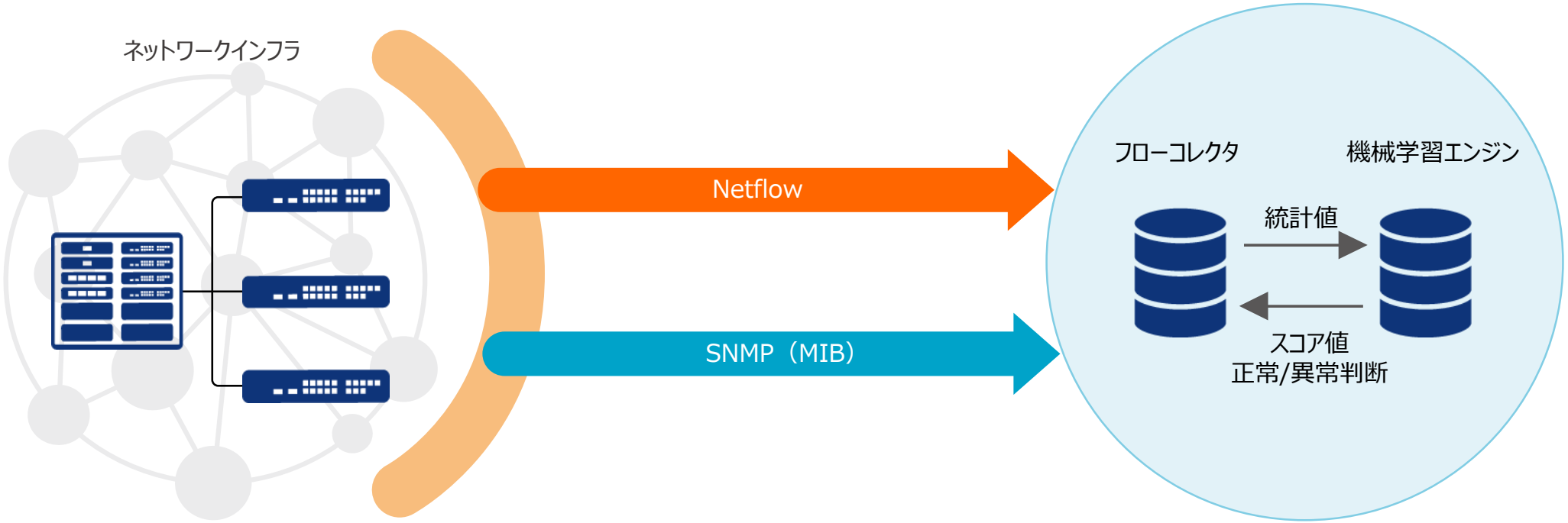


従来のような閾値監視では、閾値に届かないため、検知不可

netflowやMIBで取得した統計値と機械学習を組み合わせてることで検知可能に

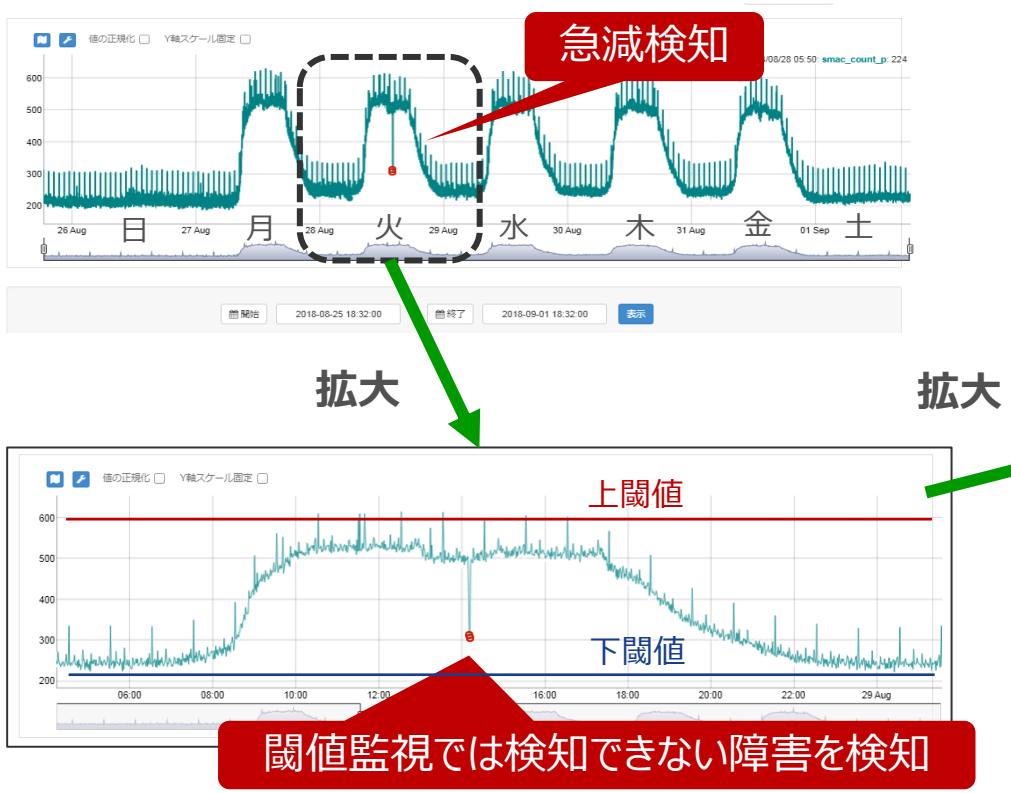
構成例

フローコレクタが、ネットワークインフラの機器から、NetflowやSNMP(MIB)を用いて情報を定期的に収集
機械学習エンジンは、統計値等から、モデルを生成。モデルと取得された統計値等から、スコア値を計算



急減を検知した例

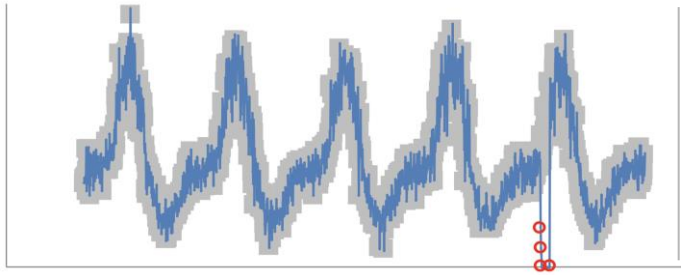
瞬断となった事象を検知し、調査対象の可能性を示唆
　火曜日の日中帯に瞬断が発生した例



- ✓ 数分の間に瞬断が２回発生
- ✓ 当該回線を調査対象とする可能性を示唆
- ✓ その後のアクションとして機器やケーブルの確認を検討できる

機械学習の応用例

周期性崩れ

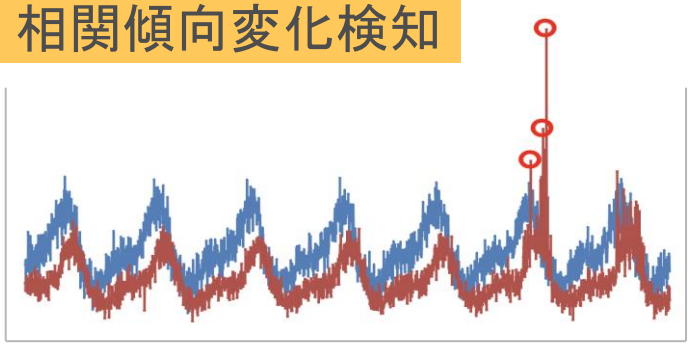


- トラフィック急減
- セッション数の落ち込み
- DDos攻撃への適用

■ 周期性を持つトラフィックや機器の情報を、過去の周期性と照らし合わせて異常を検知

- ✓ 平日日中なのにトラフィックが落ちている
- ✓ 休日なのにトラフィックが急増している

相関傾向変化検知

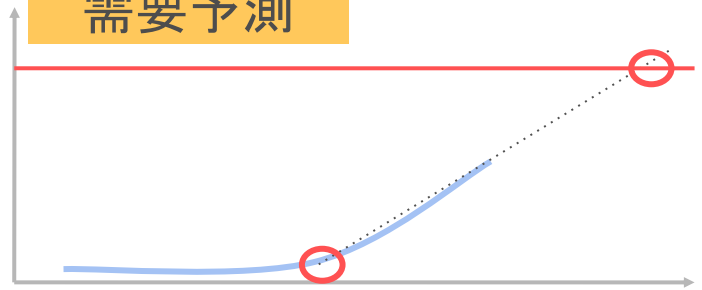


- 負荷分散されたポートのトラフィック急減
- 対向のポート間 In/Outの相関崩れ
- 対向のポート間 In/Outの相関崩れ

■ 相関傾向の異常から、故障や不具合を検知

- ✓ 並列パケット処理エンジン性能のズレ
- ✓ リンクアグリゲーション回線性能のズレ

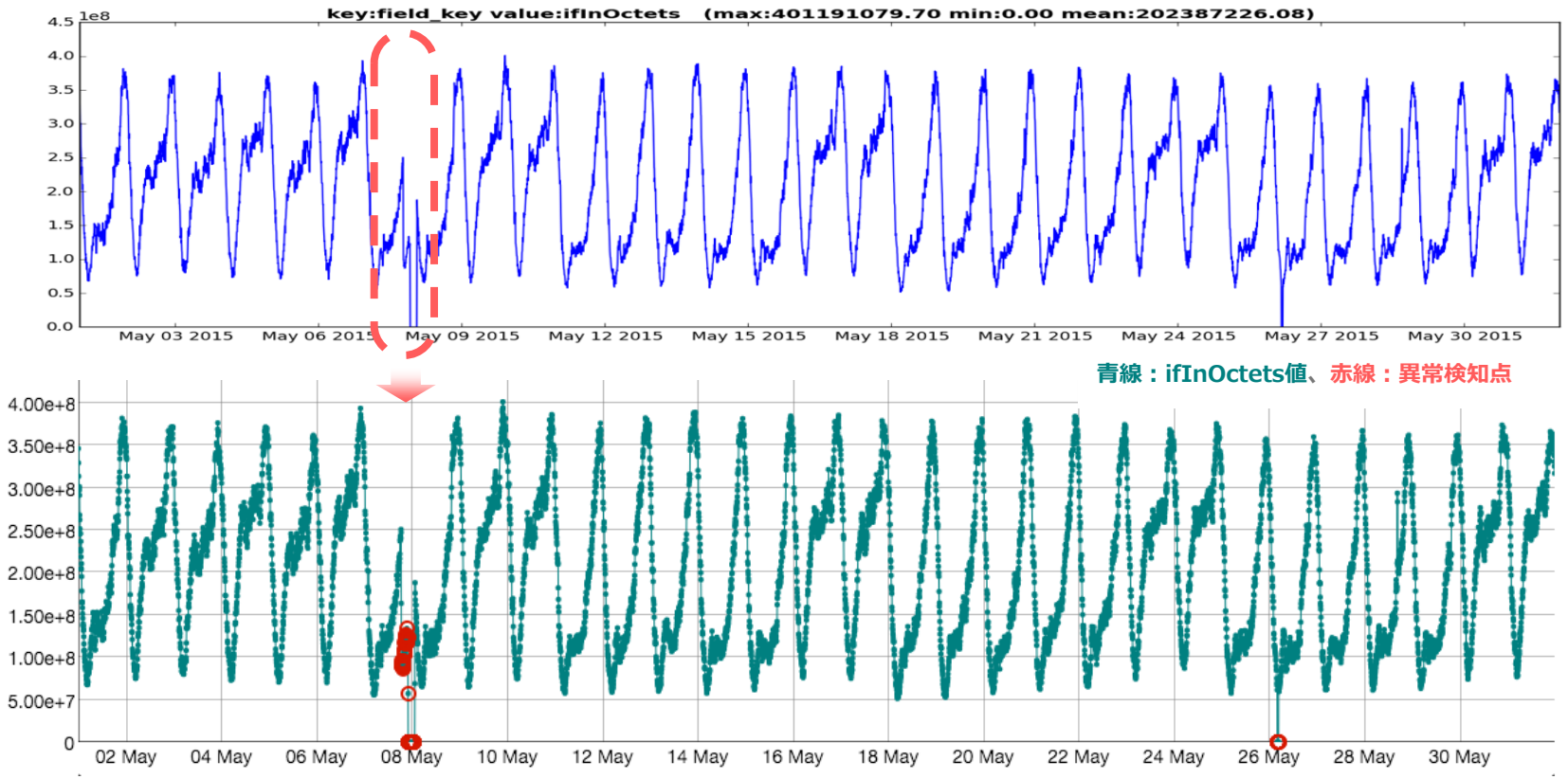
需要予測



- 仮想基盤のリソース増強タイミング予測
- ネットワーク機器の増設タイミング予測

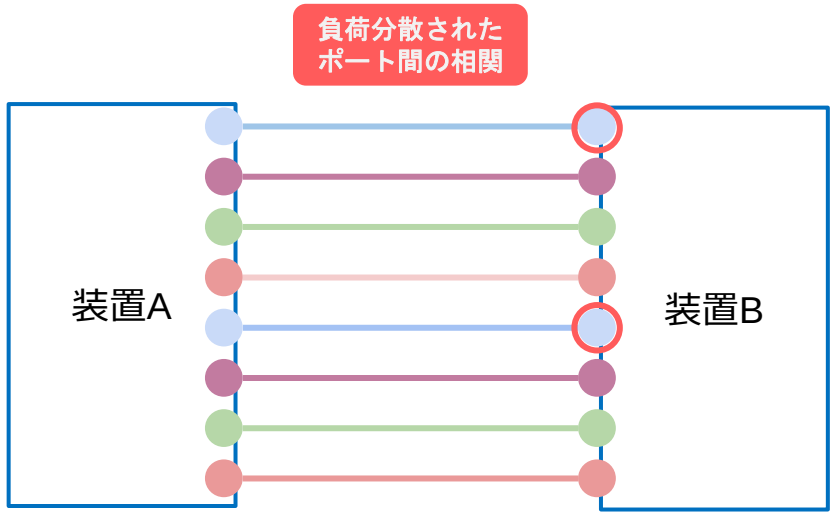
周期性崩れの例

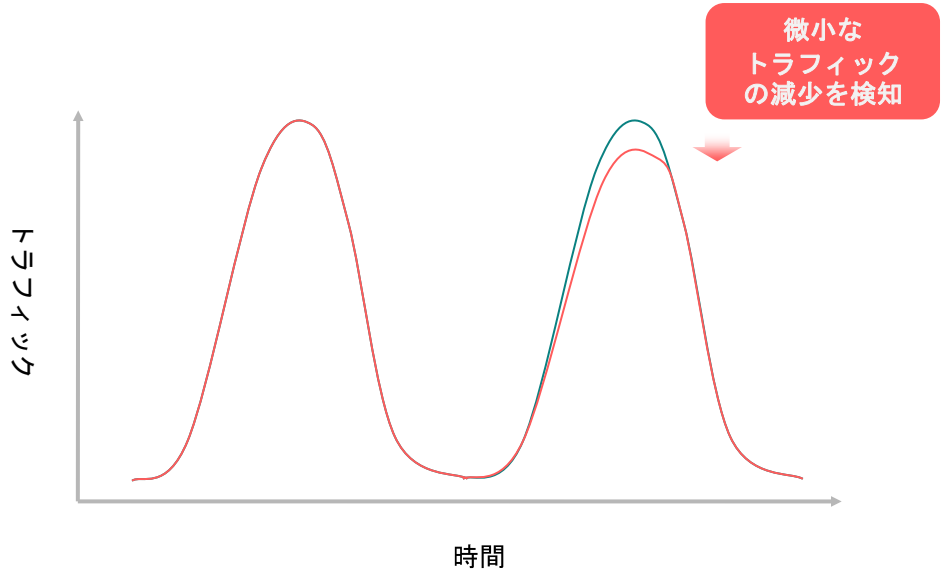
- トラフィック量の急減を検知
  - ✓ セッション数などの監視も可能



相関関係崩れの例

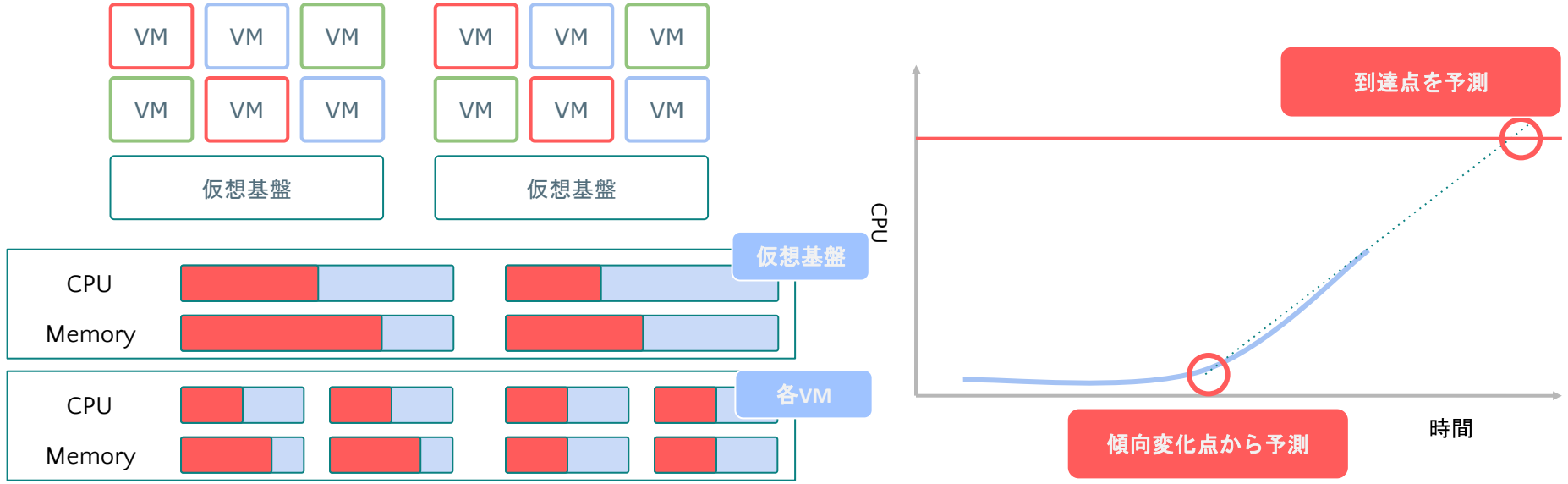
LinkAggregationなどを用いて、負荷分散を行っている複数のポートのトラフィック量を学習した相関モデルを活用。
ポート毎の偏りを監視（あるポートだけ、突然トラフィックが流れなくなった etc.）



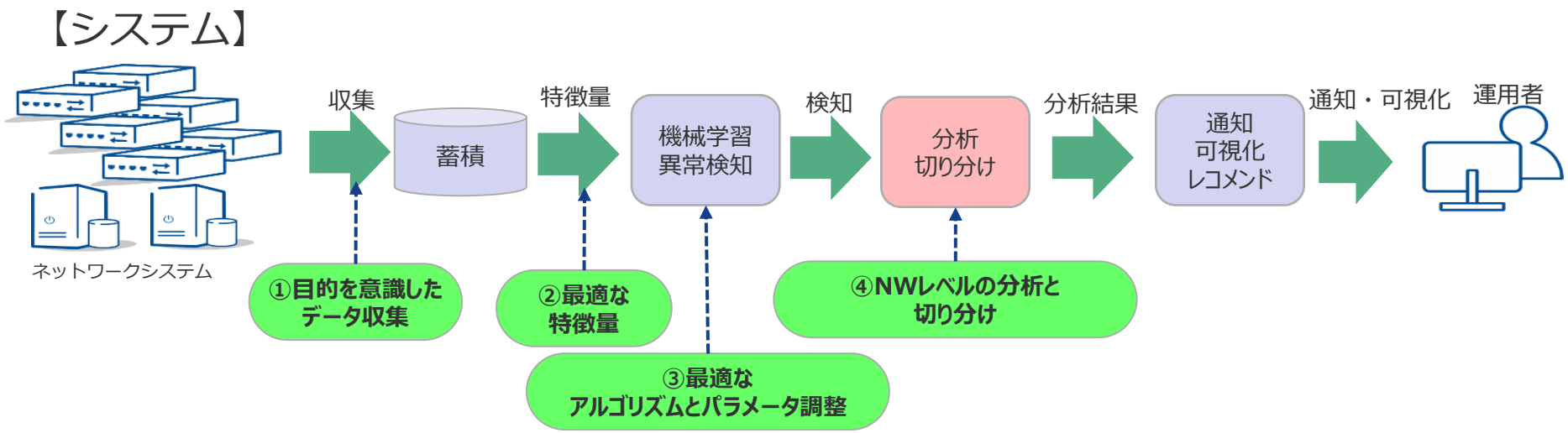


機器の需要予測

アプリケーションの要求したリソースと、実際の使用量の可視化を行い、過剰リソースの適正化
過剰リソースの削減に伴う機器増強による設備投資の抑制なども可能



どのように導入・運用するか？



①目的を意識したデータ収集
　　何を見つける必要があるのかを明確にし、それに必要なデータを収集する
②最適な特徴量
　　収集したデータを分析し、データ特性を検討する
③最適なアルゴリズムとパラメータ調整
　　周期や相関といったアルゴリズムを決定し、アルゴリズムの細かいパラーメータを調整する
④分析と切り分け
　　検知結果をもとに、分析や原因の切り分け、特定などを実施