【redmine.tokyo第27回勉強会発表資料】

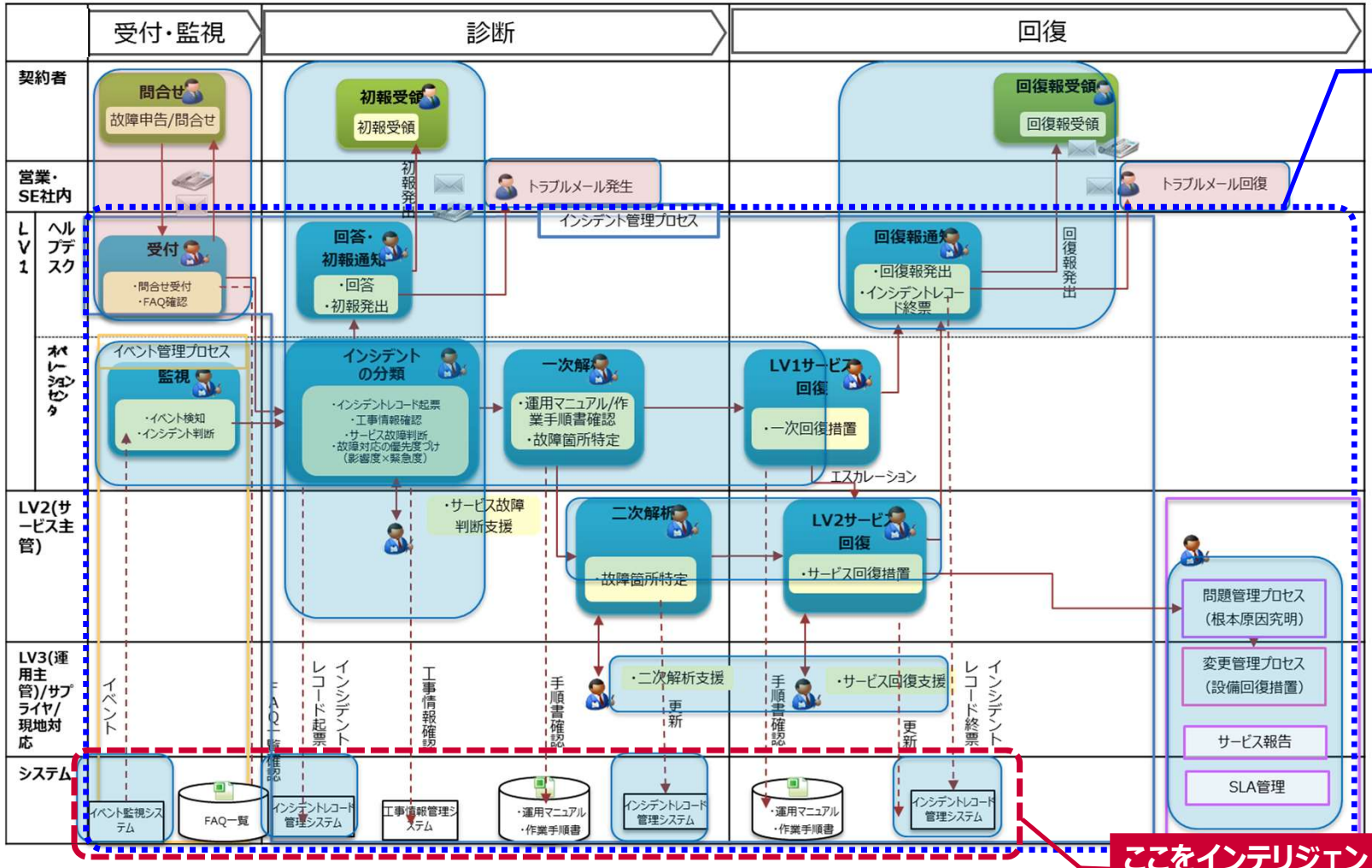
続・Redmineデータのグラフデータ化により システム監視・運用業務を効率化

～ 関連チケットの可視化、類似チケット・障害対処のレコメンド ～

2024年11月9日
NTTコムウェア株式会社
ネットワーククラウド事業本部NWソリューション部TNX-BU

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

1．システム監視・運用・保守業務の現実と理想
1－1．システム監視・運用・保守業務の例



システム監視・運用・保守業務効率化のターゲット

L1・L2・L3の役割

L1の業務

システム障害によるアラートを監視し、インシデントチケットの発行、管理、システムの正常性確認、L2へのエスカレーション

L2の業務

L1の支援やL1からのエスカレーションを受け、一次解析、サービスの正常性確認、L3へのエスカレーション、ユーザ対応

L3の業務

L2の支援やL2からのエスカレーションを受け、故障解析や故障復旧、サービス回復、今後に向けての本格対処の検討、実施

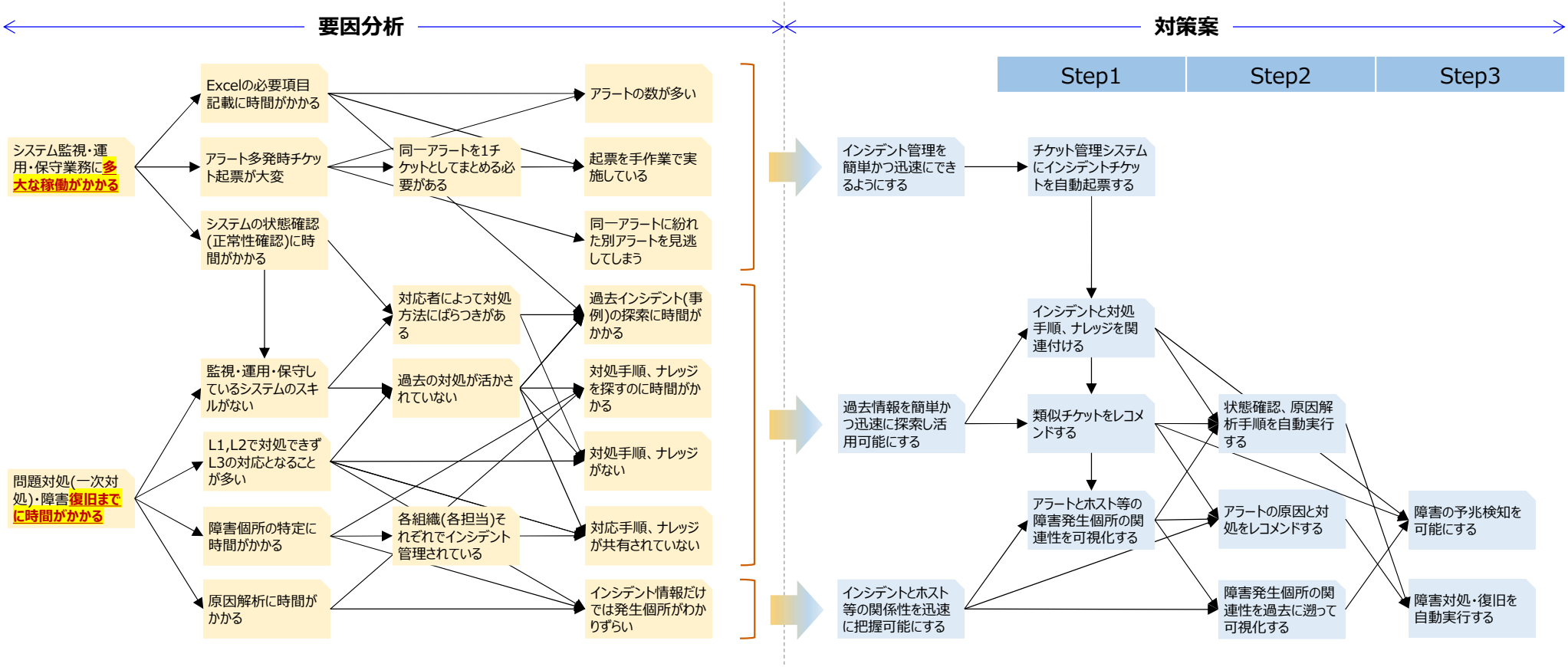
ここをインテリジェントに格好よく、スマートに実現したい！

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

1．システム監視・運用・保守業務の現実と理想
1-2．要因分析

我々はL3の役目を担っているが、L1、L2にもヒアリングし、「**システム監視・運用・保守業務はいったい何が大変なのか**」一緒に考え、2つの問題について要因分析を実施

- **システム監視・運用・保守業務に多大な稼働がかかる**
- **問題対処(一次対処)・障害復旧までに時間がかかる**



Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

1．システム監視･運用･保守業務の現実と理想
1-3．As-is･To-beの明確化

- **チケットドリブン(Ticket Driven)**
  インシデントや問題に対して、チケット駆動によりアクションが実行されることで、作業内容が記録され対応手順等のナレッジが蓄積される
- **グラフデータサイエンス(Graph Data Science)**
  情報の複雑な関係性や依存関係を可視化したり、グラフデータサイエンスの活用により、問題の発生個所や解決策のレコメンドが可能となる
- **AI(Artificial Intelligence)**
  AIの導入によりインテリジェントなシステムが構築可能で、グラフデータサイエンスと合わせ、障害の予兆検知、自律的な障害復旧が期待できる
- **自動化(Automation)**
  作業プロセスや手順の自動化により、反復的な作業や定型業務を効率的に処理し、人的エラーを減少させることができる

４つのアプローチ

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

2．To-be実現ステップの検討

Step1：チケット自動起票とチケットの活用

- システム監視によるアラートをインシデントチケットとして自動起票
- 各種対応をITILベースで体系化したチケットとして管理(右図)し活用
- インシデントチケット間やホストチケットの関係性も含め、これらのチケットの関連を可視化

Step2：原因解析と対処を高度にサポート

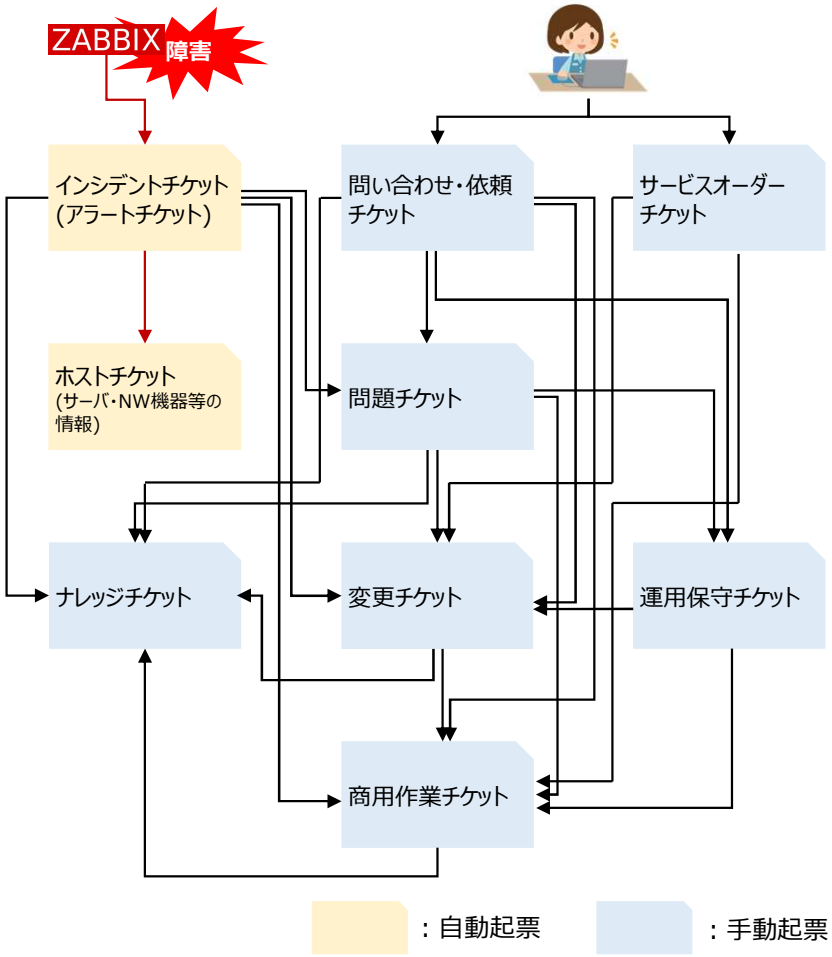
- システム状態の自動確認と原因解析手順の自動実行により、問題の根本的な要因を素早く特定
- 蓄積された過去情報からレコメンドされた原因や対処手段を得ることで障害復旧を迅速に行うことが可能
- 障害発生状況を時系列で可視化することにより、障害の連鎖を把握

Step3：インテリジェントな予兆検知と自律回復

- 障害の予兆を検知し、問題が発生する前にアクションを起こし対処することで、障害を未然に防止
- 自律的な対処手順の立案、そして、その手順に従った対処を自律的に実行し障害復旧を自動で実施

：今回実現した範囲

ITILベースのチケット管理



Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

3．システム監視・運用・保守業務の効率化
3-1．RedmineとグラフDBを活用したシステム運用業務のイメージ

ZABBIX ※1

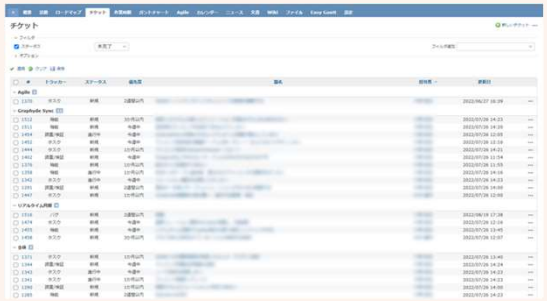
①インシデントチケット・ホストチケット自動起票

REDMINE
flexible project management

PostgreSQL
RDB

システム監視

インシデント管理・システム運用管理



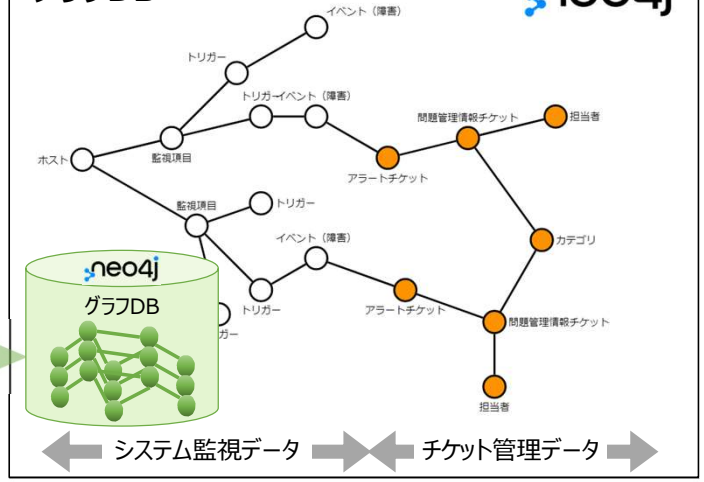
Graphyde Sync ※2

②チケットデータをグラフデータ化

インシデントチケット

③システム運用業務にグラフデータを活用

グラフDB ※3



①インシデントチケット・ホストチケット自動起票

システム監視ツールであるZABBIXで検知したアラートをインシデントチケットとして、ホストチケットとともにチケット管理ツールであるRedmineにAPIを利用して自動起票する

②チケットデータをグラフデータ化

次にRedmineのRDBに格納されたチケットのデータをグラフデータ化する

③システム運用業務にグラフデータを活用

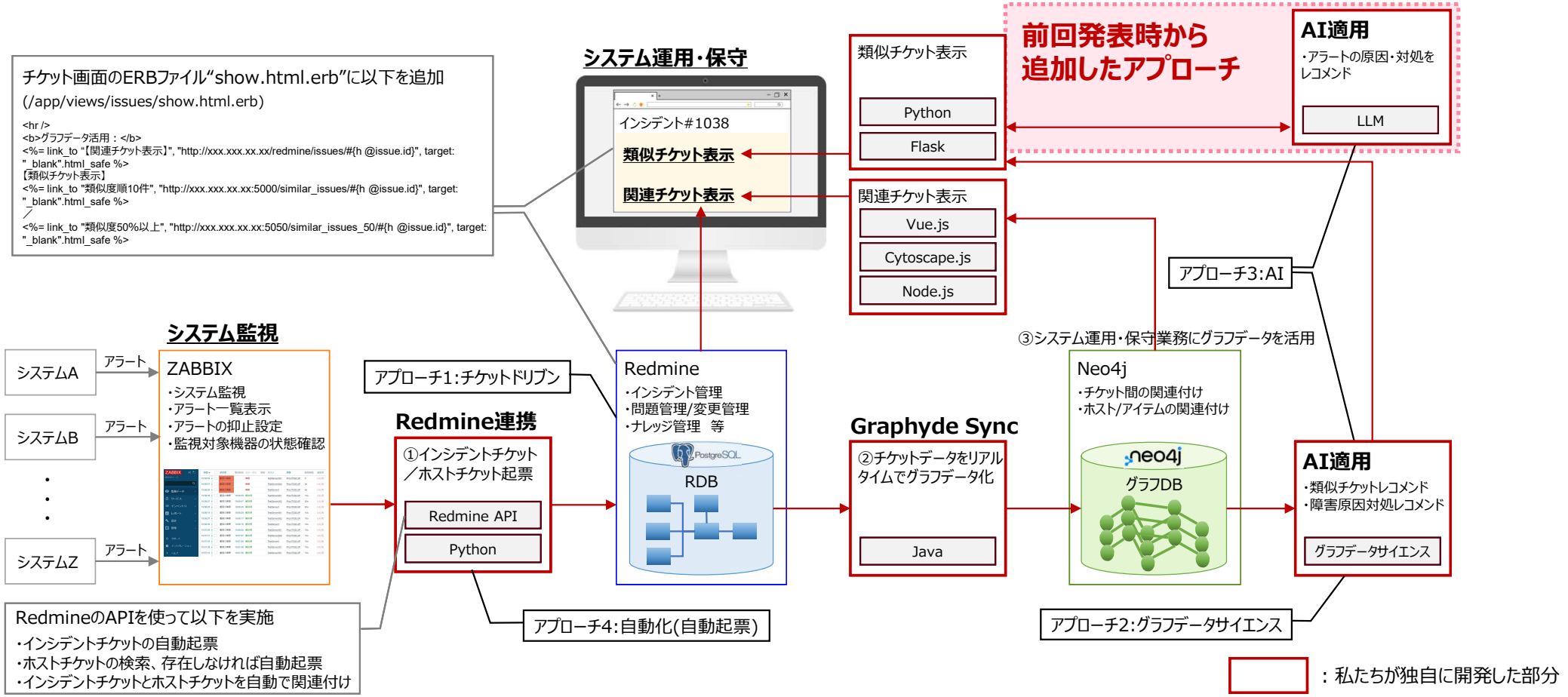
そして、グラフDBに格納されたデータを活用して、「関連チケット表示」や「類似チケット表示」を実現する

※1：Zabbixは、サーバ、ネットワーク、アプリケーションを集中監視するためのオープンソースの統合監視ソフトウェア。監視、障害検知、通知機能を備えており、シンプルで使いやすいため、世の中で広く利用されている。
※2：Graphyde Sync ® は、私たちが開発した「コーディングレスでRDBのデータをリアルタイムでグラフDBに連携」する世界でも類をみないRDBとグラフDBの連携ソリューション。
※3：グラフDBは、グラフ理論に基づくグラフ構造に最適化されたデータベースで、グラフデータサイエンス技術を利用するために必要なグラフ化されたデータを保持する。製品としてはNeo4jが圧倒的シェアを誇っている。

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

3．システム監視・運用・保守業務の効率化
3-2．4つのアプローチによるシステム監視・運用・保守アーキテクチャ

- 4つのアプローチ(チケットドリブン、グラフデータサイエンス、AI、自動化)を用いて実現したシステム監視・運用・保守の仕組み



Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

４.システム監視・運用・保守の効率化デモ

・関連チケット表示

・類似チケット表示

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

5．実現効果の確認（1／2）

某システムの2023年12月のアラート発生状況(既存63件・新規10件)から稼働を算出し、提案手法適用後の効果をシミュレーションした結果

システム監視・運用・保守業務における L1・L2・L3の役割	現状							提案手法適用後							
	作業内容	既存アラート			新規アラート			作業内容	既存アラート			新規アラート			
		対応件数	稼働(h)	復旧時間	対応件数	稼働時間	復旧時間		対応件数	稼働(h)	復旧時間	対応件数	稼働時間	復旧時間	
L1 システム監視	・対応マニュアル探索し対処方法確認 ・システム正常性確認 ・Excelのインシデント管理簿にアラート内容、システム正常性確認結果記載 ・TeamsでL2連絡、情報共有	63	42.0	42.0	10	6.7	6.7	・類似チケット検索し対処方法確認 ※類似チケットの対処内容を確認しシステム正常性確認OKならL2連絡不要 ・システム正常性確認 ・インシデントチケットにシステム正常性確認結果記載 ※アラート内容の記載はチケット自動起票時記録されるため不要 ※チケット共有のためL2連絡不要	63	13.7	13.7	10	2.2	2.2	
L2 一次解析・一次対処 ※定期メンテナンス作業、アクション会議、ユーザ対応等の稼働は除く	・対応マニュアル探索し対処方法確認 ・サービス正常性確認 ・Excelのインシデント管理簿にサービス正常性確認結果記載 ・TeamsでL3連絡、情報共有	63	47.3	47.3	10	7.5	7.5	・類似チケット検索し対処方法確認 ※類似チケットの対処内容を確認しサービス正常性確認OKならL2連絡不要 ・サービス正常性確認 ・インシデントチケットにサービス正常性確認結果記載 ※チケット共有のためL3連絡不要	31.5	16.3	16.3	10	5.2	5.2	
L3 故障解析・故障復旧 ※本格解析・本格対処、アクション会議、問い合わせ対応、改善等の稼働は除く	・インシデントチケット起票 ・サービス影響判断、故障解析、復旧 ※解析、復旧作業は複数人で実施 ・解析、対処内容をチケットに記載 ・TeamsでL1、L2連絡、結果共有	63	78.8	47.3	10	31.7	15.6	※インシデントチケットは自動起票のため手動起票不要 ・サービス影響判断、故障解析、復旧 ※類似チケットの解析・対処内容把握、LLMによる原因、対処を参考に実施 ※解析、復旧作業は複数人で実施 ・解析、対処内容をチケットに記載 ※チケット共有のためL1、L2連絡不要	6.3	3.7	2.1	10	17.0	9.0	
	2023年12月分の合計時間(h)		168.0	136.5		45.8	29.7	想定合計時間(h)		33.6	32.0		24.3	16.3	
	1件当たりの平均時間(h)		2.7	2.2		4.6	3.0	1件当たりの想定平均時間(h)		0.5	0.5		2.4	1.6	

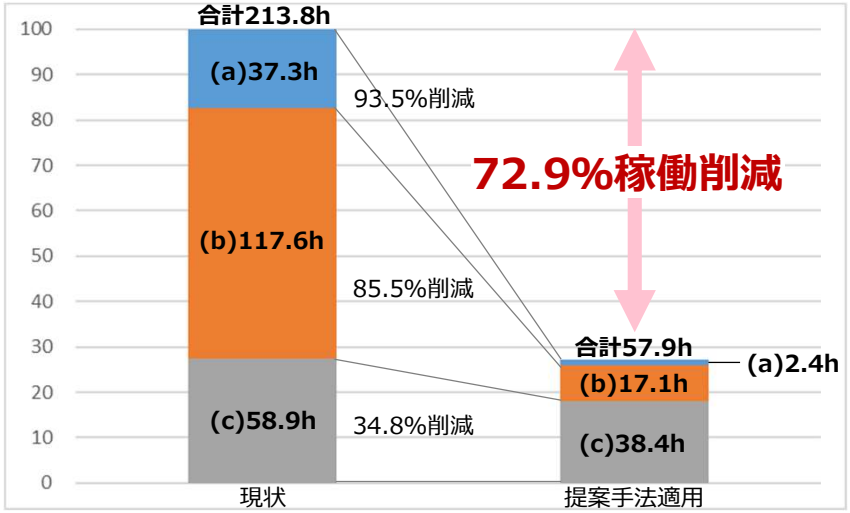
共有されたチケットの情報・類似チケット表示から適切な情報を得ることで、半分(1/2)程度はL2へのエスカレーションなしでOKと判断されることを想定

類似チケットで表示した解析結果・対処内容の情報が不十分なため、L3に問い合わせることが1/5程度はあると想定

5．実現効果の確認（2／2）

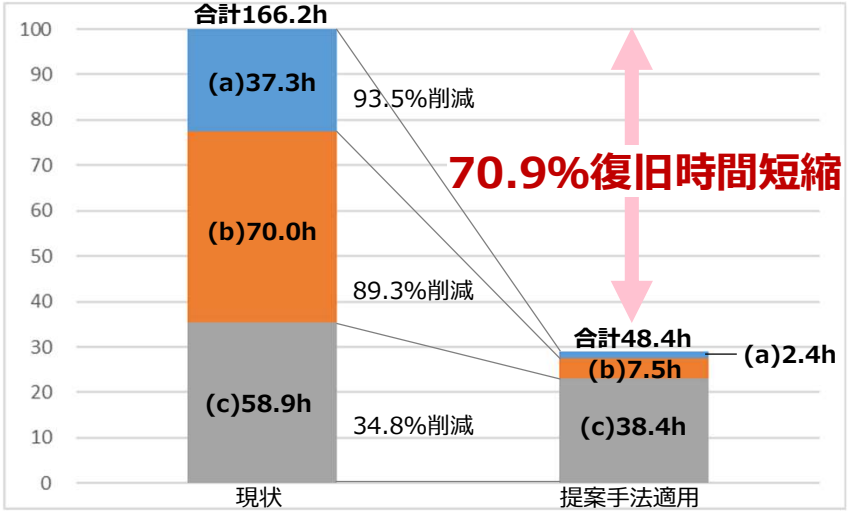
● 稼働削減効果
213.8時間→57.9時間に削減　72.9％稼働削減

既存・新規アラート対処の現状稼働時間213.8hを100%とした場合の効果



● 復旧時間短縮効果
166.2時間→48.4時間に短縮　70.9％復旧時間短縮

既存・新規アラート対処の現状復旧時間166.2hを100%とした場合の効果



(a) チケット自動起票・チケット管理による情報共有効果
Excelによるインシデント管理は、チケット自動起票により不要となり、L1、L2、L3の情報連携もすべてチケットによる共有となるため、Teamsによる連絡も不要となる。

(b) 関連チケット表示・類似チケット表示によるレコメンド効果
類似チケットから対処内容を把握することが可能になるため、マニュアル探索が不要で、適切な対処内容がレコメンドされることにより、L1→L2→L3へのエスカレーションを大幅に減らすことができ、L3においては、関連チケット表示によるアラートの集中や連鎖の把握、LLMによる原因と対処のレコメンドは、故障解析時間が短縮される。

(c) その他、副次的効果
システムおよびサービスの正常性確認、その結果の記録はこれまでと変わらないが、L2、L3の対応件数が減ることにより稼働の削減と復旧時間を短縮することができる。

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

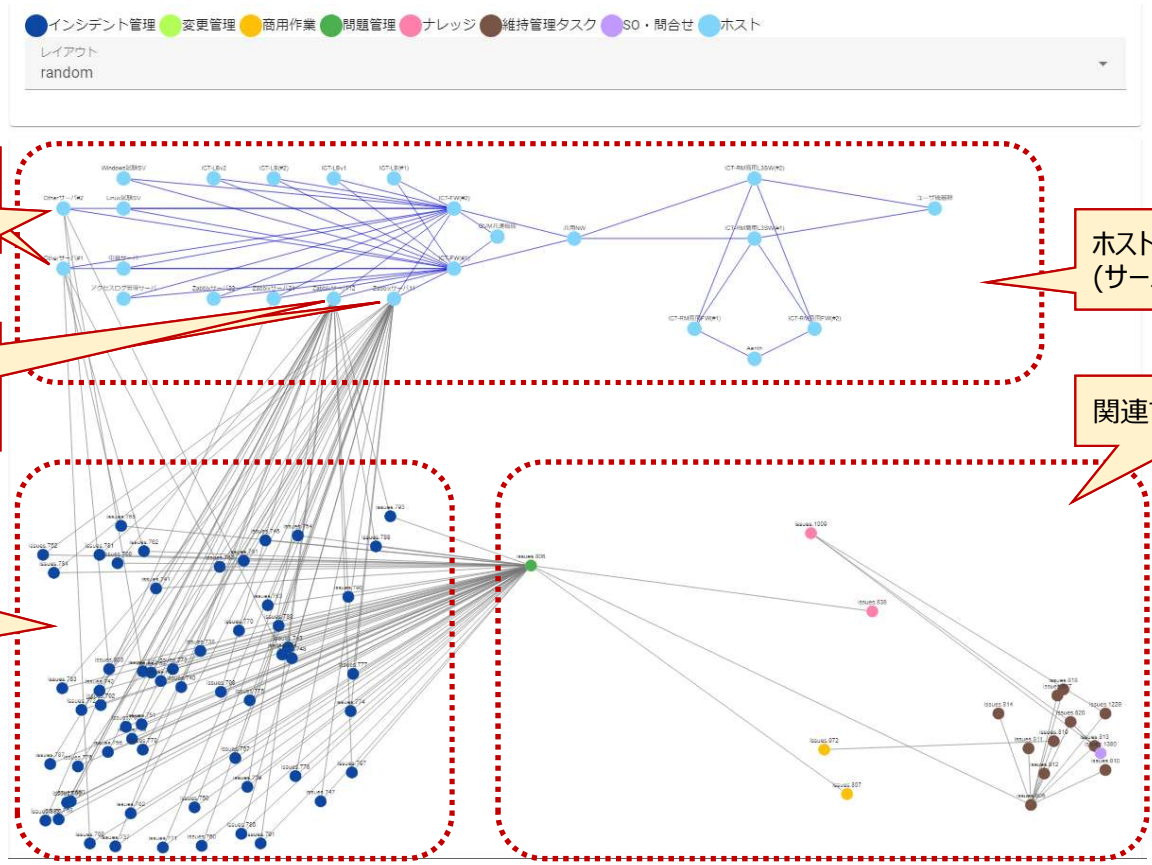
ご清聴ありがとうございました

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

【参考】「関連チケット表示」の画面例

- インシデントチケットをはじめ各プロジェクトのチケットデータをグラフデータ化することで、その関係性を以下のように表すことが可能

関連チケット表示



- アラートにより起票されたインシデントチケット(発生アラート)とホストチケットをグラフDBで紐づけ
- それにより、障害が発生時、どこのホストで発生したアラートか、アラートが集中している個所はどこか、視覚的かつ即座に判別可能

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY

【参考】「類似チケット表示」の画面例

- 各プロジェクトのチケットデータをグラフデータ化し、AI技術を活用することで、原因・対処のレコメンド、類似チケットの抽出が可能

類似チケット表示

Issue ID	Issue Subject	Issue Description	Similarity Rate
1038	[przabbix21]Zabbix Server log/Zabbix Server error:ERROR	[イベント発生時刻]2023-07-13 19:57:14.002195819 [アラート内容]4055481:20230713:195622.270 Failed to execute command ¥"/bin/traceroute 10.166.110.250¥": Timeout while executing a shell script. [イベント詳細URL]http://prictrmclma.icp.gvm-jp.groupis.ntt/zabbix/tr_events.php?triggerid=70437&eventid=54655	100.00%

注：LLMの応答結果

[原因]
Zabbixサーバーが"/bin/traceroute 10.166.110.250"というコマンドを実行しようとしましたが、タイムアウトが発生しました。tracerouteコマンドが応答しなかった可能性があります。

[対処]
以下の手順を試してみてください。

1. tracerouteコマンドが正しくインストールされているか確認してください。コマンドラインで「traceroute」と入力し、正常に実行されることを確認してください。もしインストールされていない場合は、適切なパッケージをインストールしてください。

2. ネットワーク接続に問題がある場合は、ネットワーク接続を確認してください。tracerouteコマンドは、指定したアドレスにパケットを送信して経路をトレースするため、ネットワーク接続が必要です。

3. タイムアウト値を調整してみてください。Zabbixの設定ファイルであるzabbix_server.confで、Timeout=値（デフォルトは3）を適切な値に変更してみてください。タイムアウト値を長くすることで、応答が遅い場合でもコマンドの実行を継続させることができます。

4. 他のネットワークトラブルシューティング手法を試してみてください。tracerouteコマンドがタイムアウトする原因が他の要因である可能性もありますので、他のシステムログやネットワーク設定をチェックしてみてください。

なお、以下の類似チケットに対処のヒントがあるかもしれません。
- [ZBXNEXT-6749] - Timeout <secs>_when executing agent_dusk.sh with denormalised number of digits on value_map.

Similar Issue ID	Similar Issue Subject	Similar Issue Description	Similarity Rate
1108	[przabbix21]Zabbix Server log/Zabbix Server error:ERROR	[イベント発生時刻]2023-07-31 15:53:14.003173708 [アラート内容]4055746:20230731:155249.491 Failed to execute command ¥"/bin/traceroute 10.188.162.26¥": Timeout while executing a shell script. [イベント詳細URL]http://prictrmclma.icp.gvm-jp.groupis.ntt/zabbix/tr_events.php?triggerid=70437&eventid=199622	90.43%

Associated Issue ID	Associated Issue Subject	Associated Issue Description

1153	zabbix_serverログのping/traceroute実行結果エラーに関するアラートの除外設定	■変更内容
		zabbix_server.logの監視アイテムに以下のキーワードで除外設定を追加する。
		<pre>
		Failed to execute command
		</pre>
		■変更理由
		該当メッセージはZabbixの画面から設定されたホストに対してping等コマンドを実行してエラーとなった際に発生するメッセージである。
		コマンド実行結果は画面表示されるので、ログ検知は不要であるため除外設定を行う。
		!clipboard-202308071319-ezlkc.png!

LLMを活用してインシデントチケットの内容(アラート)に対する原因・対処をレコメンド

グラフデータサイエンスを活用して類似チケットをレコメンドするとともに関連チケットを表示し対処内容をレコメンド

- インシデントの対応時、AI技術を活用し、類似する関連チケットを抽出するとともにアラートの原因・対処をレコメンド
- それにより、迅速な原因解析、適切な対処・対応が可能

Copyright © NTT COMWARE CORPORATION 2024
NTT COMWARE CORPORATION CONFIDENTIAL PROPRIETARY