

# Zabbixへのマイグレーションと アップデートによる運用効率化

2024年11月22日

NTTコムエンジニアリング株式会社

大西 勘太郎

# 自己紹介

氏名 : 大西 勘太郎

所属 : NTTコム エンジニアリング株式会社  
スマートオペレーションサービス部  
オペレーションマネジメント部門

出身 : 千葉県流山市

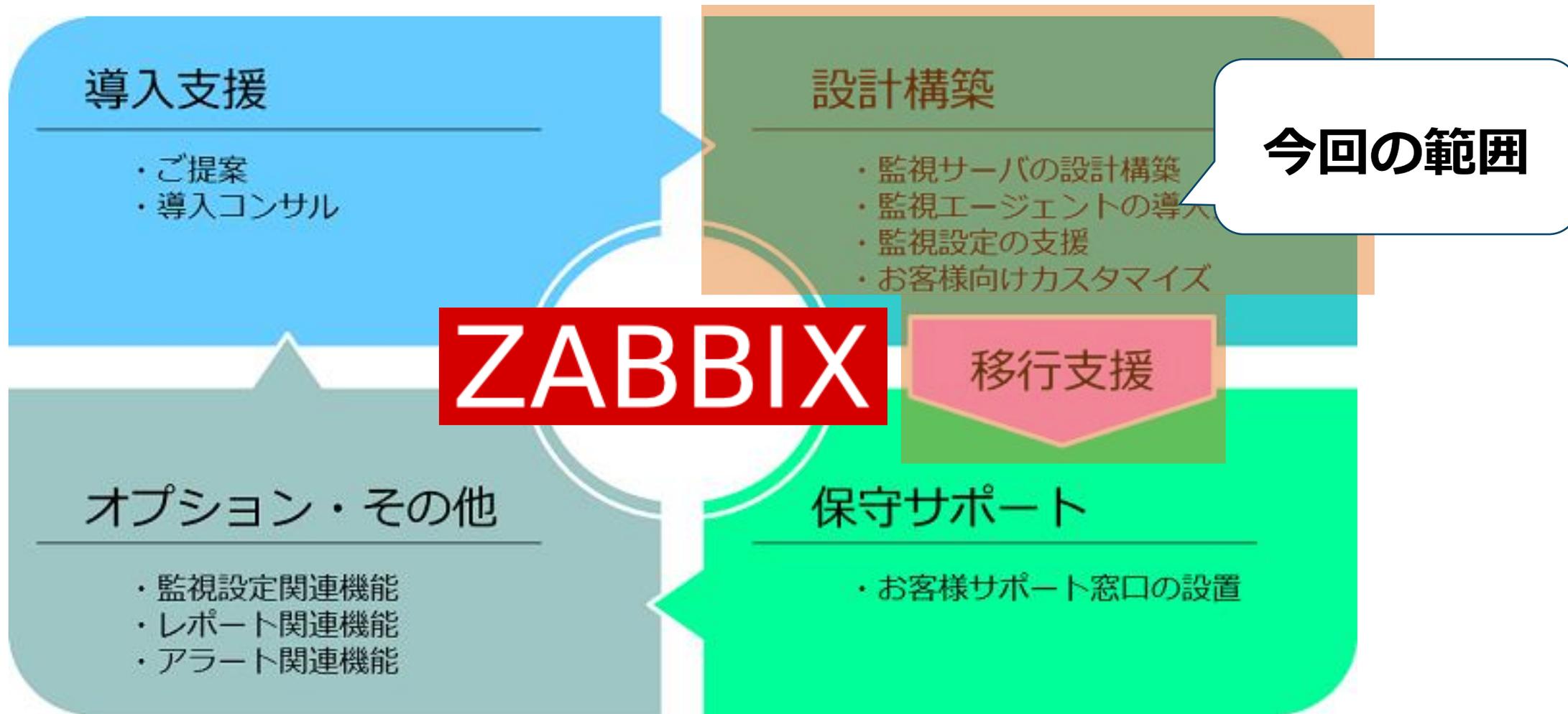
経歴 : 2019年 NTTコムソリューションズ入社  
Zabbix関連部署に配属  
システム監視の提案・構築の業務に従事  
2022年 Zabbix Conference Japanで登壇（リモート）  
Zabbix認定技術者（スペシャリスト）



## NTTコム エンジニアリング株式会社

- NTTコミュニケーションズグループにて、提案 / 設計構築 / 保守運用を担うVC子会社
- 自社の製品/サービスは「docomo Business」ブランドにて提供
- NTTコミュニケーションズまたはドコモビジネスソリューションズより販売
- Zabbix関連ソリューション事業「**ZABICOM**」を提供





# マイグレーションとアップデート

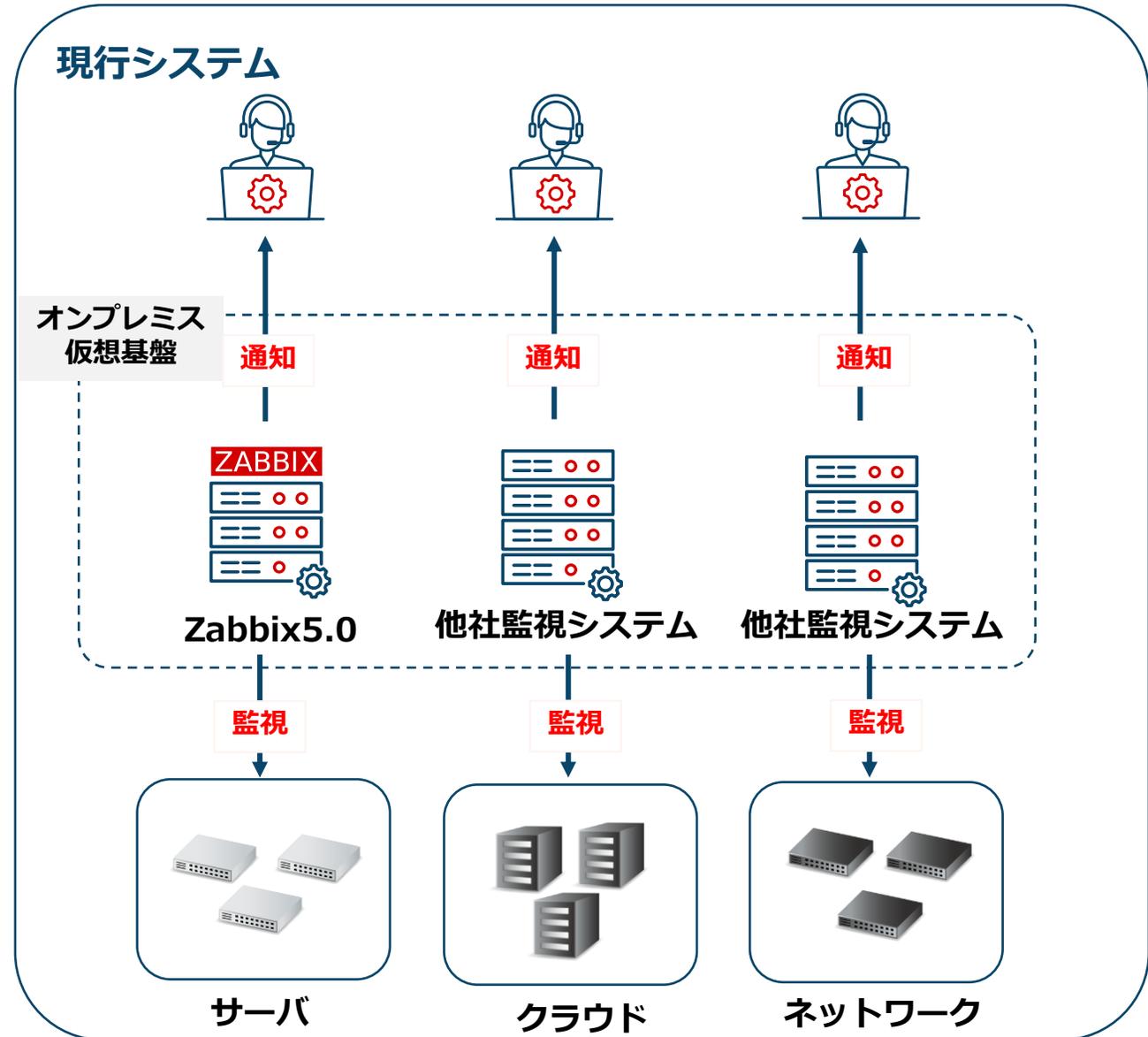
# 今回ご紹介する事例（マイグレーションとシステム統合）

## ◆概要

- 現行環境：複数の監視システムを並行利用
- 監視対象：サーバ、クラウド、ネットワーク
- 監視台数：1000台以上

## ◆課題

- 監視システムごとに操作性が異なる
- システム毎に監視の基準が異なる
- システム全体を俯瞰した監視が出来ていない
- チーム間での情報共有が難しい
- 一部システムのOSがEOLを迎えている



# 今回ご紹介する事例（マイグレーションとシステム統合）

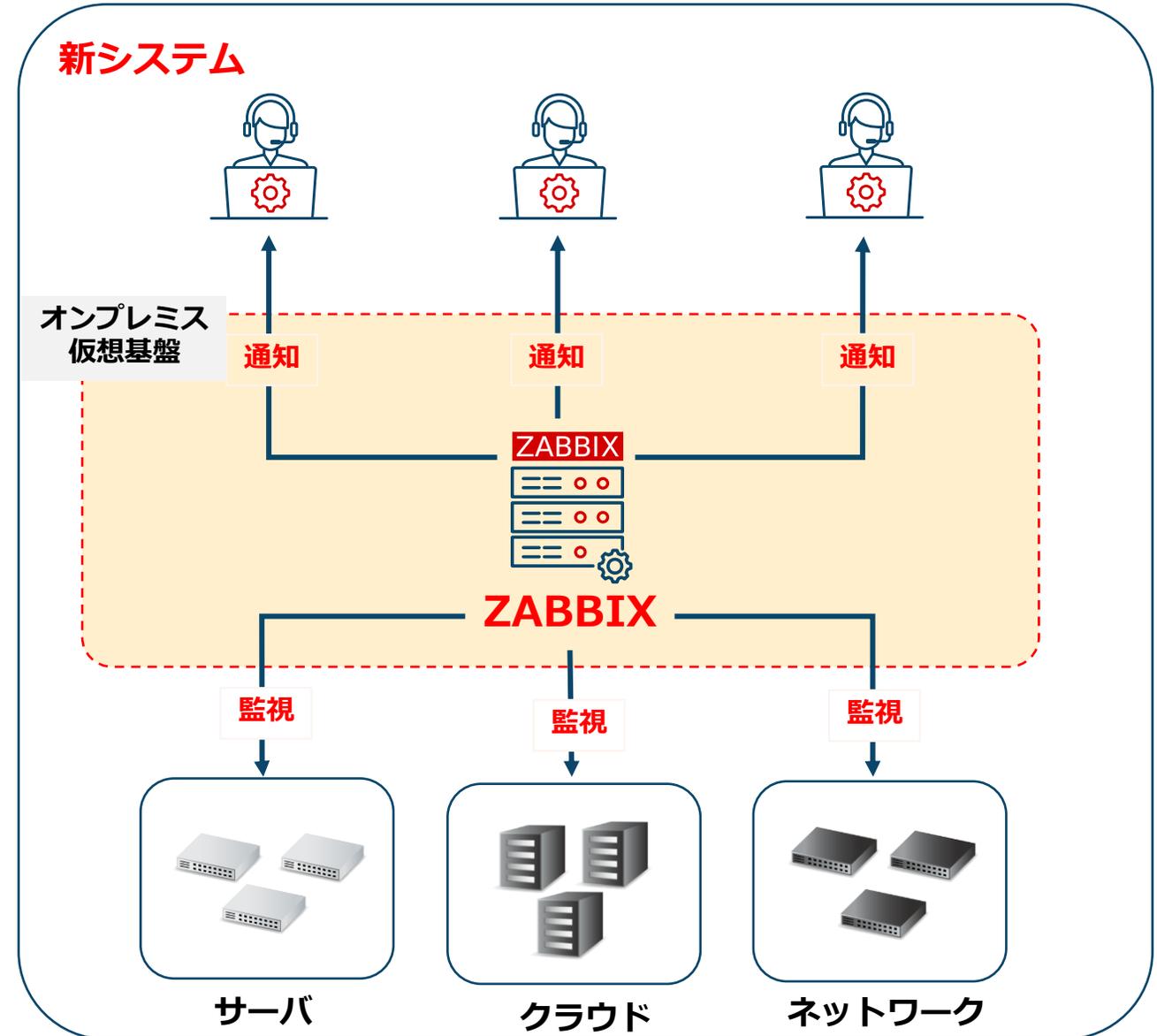
## ◆要件

- 目的 : 課題点の解消
- 導入環境 : オンプレミス仮想基盤
- 耐用年数 : 5年
- 構築期間 : 6か月以内

## ◆課題解決

- 監視システムごとに操作性が異なる
- システム毎に監視の基準が異なる
- システム全体を俯瞰した監視が出来ていない
- チーム間での情報共有が難しい
- 一部システムのOSがEOLを迎えている

→監視システムをZabbixに一元化し、  
運用オペレーションの課題を解消



# Zabbixアップデート

# アプリケーションレベルのアップデート

## メリット

- インターネット上のリポジトリからパッケージを用いたアップデートが可能

## デメリット

- OSのEOLに対応できない
- OSのバージョンによってはミドルウェアのバージョンが適合しない



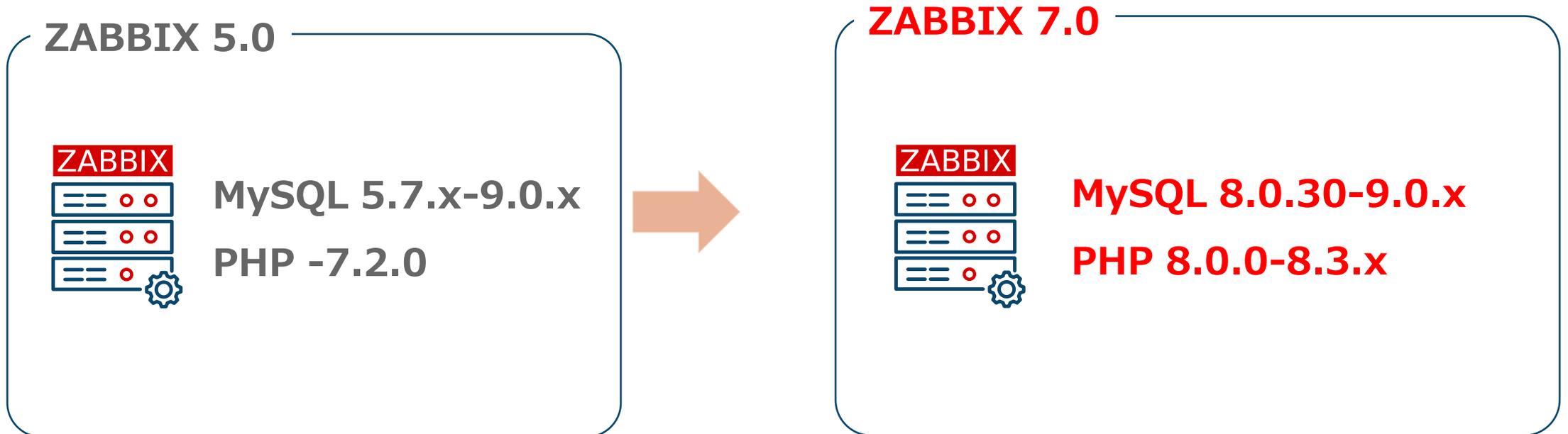
# OSレベルでのアップデート

## メリット

- OSのEOLに対応
- OS標準リポジトリでZabbixの動作要件を満たせる

## デメリット

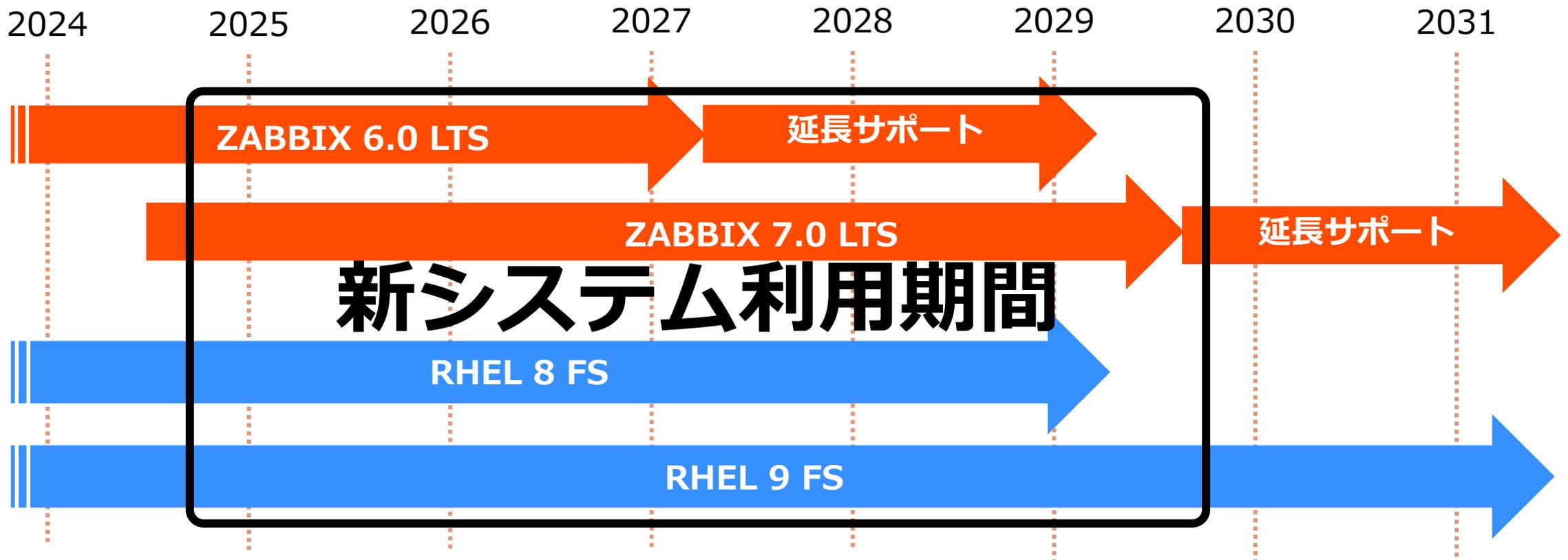
- システム停止を伴う更改が必要



# OSレベルでのアップデート

- RHEL7はEOL、その他ミドルウェアも7.0の必要バージョンを満たしていない
- 新システムの耐用年数は5年

→OSレベルでの再構築に決定



# Zabbix7.0 アップデートにおける課題

# 課題①現状の設定に囚われてしまう

- 新パラメータの追加が行われている場合、それに気付かない

## ZABBIX 設定ファイルのパラメータ数推移

	ZABBIX 5.0	ZABBIX 6.0	ZABBIX 7.0
パラメータ数	94	108	121
増加数	-	14	13

- バージョンアップごとに、10個以上のパラメータが追加されている

# 課題①現状の設定に囚われてしまう

- 同一パラメータでも意味が異なる場合がある
- 7.0新機能「非同期ポーラープロセス追加」によるマルチスレッド化



**-6.0**

- Zabbixエージェント
  - HTTPエージェント
  - SNMPエージェント
  - 上記以外のポーリング監視
- **StartPollers**



**7.0 New!**

- Zabbixエージェント  
→ **StartAgentPollers**
- HTTPエージェント  
→ **StartHTTPAgentPollers**
- SNMPエージェント  
→ **StartSNMPPollers**
- 上記以外のポーリング監視  
→ **StartPollers**

# 課題①現状の設定に囚われてしまう

- 同一パラメータでも意味が異なる場合がある
- 7.0新機能「非同期ポーラープロセス追加とマルチスレッド化」



~6.0

**StartPollers = 20**



7.0 New!

**StartAgentPollers = 1**

**StartHTTPAgentPollers = 1**

**StartSNMPPollers = 1**

**StartPollers = 20**

必要無量のパラメータを設定してしまっている

- 新旧の監視設定を意識したパラメータの再設計が必要

# 課題②旧Zabbix Agentの使用

## ➤ よくあるご要望

旧バージョンのZabbix Agentのまま運用したい

SERVER-AGENT間は  
**下位互換性**があるし…



システム管理者

大量のホストの  
Agentアップデートは  
**時間と労力**がかかる…

# 課題②旧Zabbix Agentの使用

➤ Zabbix7.0 「エージェントの状態」 アイコンの仕様変更

**パッシブチェック・アクティブチェック両方のステータスが「利用可能」の場合**  
「エージェントの状態」アイコンが緑になる



# 課題②旧Zabbix Agentの使用

しかし…

6.0以前のエージェントには アクティブチェックのステータス表示機能が無い

→ 「エージェントの状態」アイコンが緑にならない。



The screenshot shows the Zabbix Agent status page. At the top, there are tabs for 'エージェントの状態', 'エージェント暗号化', '情報', and 'タグ'. Below the tabs, there is a table with columns for 'インターフェース', 'ステータス', and 'エラー'. The first row shows the interface '127.0.0.1:10050' with a status of '利用可能' (green) and an error of '不明' (grey). The second row shows the active check status 'アクティブチェック' with a status of '不明' (grey). Red boxes highlight the 'ZBX' agent name and the '不明' status for the active check.

インターフェース	ステータス	エラー
127.0.0.1:10050	利用可能	
アクティブチェック	不明	

# 課題②旧Zabbix Agentの使用

「エージェントの状態」アイコンを用いて  
 エージェントとの疎通を確認している運用現場も多い  
 →現状では7.0Agentを導入するか、諦めるしかない

※諦めたくない人用

Zabbix 機能追加・改善 フォーム

→[ZABBIX FEATURE REQUESTS](#)(ZBXNEXT)



運用オペレーター

# 課題②旧Zabbix Agentの使用

➤ 旧Zabbixエージェントで使用できない機能を把握しておくことも大事

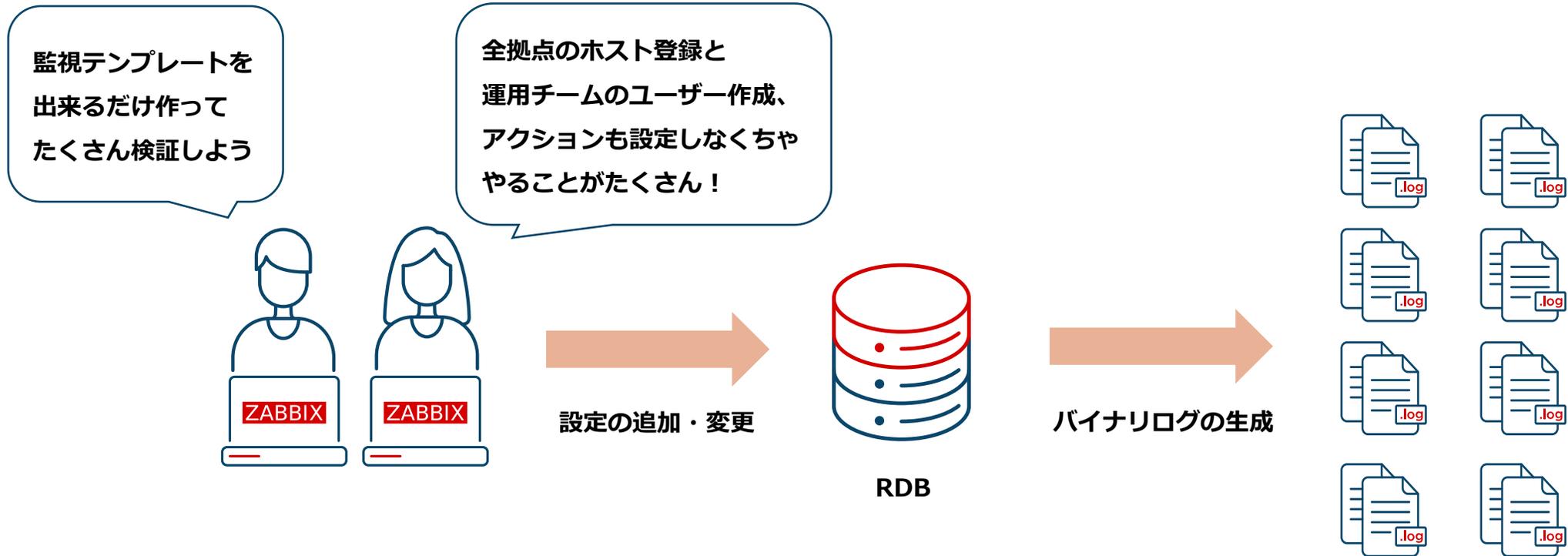
Agent	下位互換性の無い機能
1.8以前	<ul style="list-style-type: none"> <li>・ 監視アイテム…logrt</li> <li>・ ローレベルディスクカバリで使用できる標準のアイテム</li> </ul>
2.0以前	<ul style="list-style-type: none"> <li>・ Server-Agent間の暗号化通信</li> </ul>
4.0以前	<ul style="list-style-type: none"> <li>・ アイテムキーのアクセス制御 (Allowkey/Denykey)</li> </ul>
6.0以前	<ul style="list-style-type: none"> <li>・ アクティブチェックステータス表示機能</li> <li>・ アイテム単位のタイムアウト設定</li> </ul>

最新のエージェントを導入することが望ましいが、  
それが出来ない場合、**使用できない機能があることを必ずお客様にご説明する**

# 課題③ バイナリログによるディスク圧迫

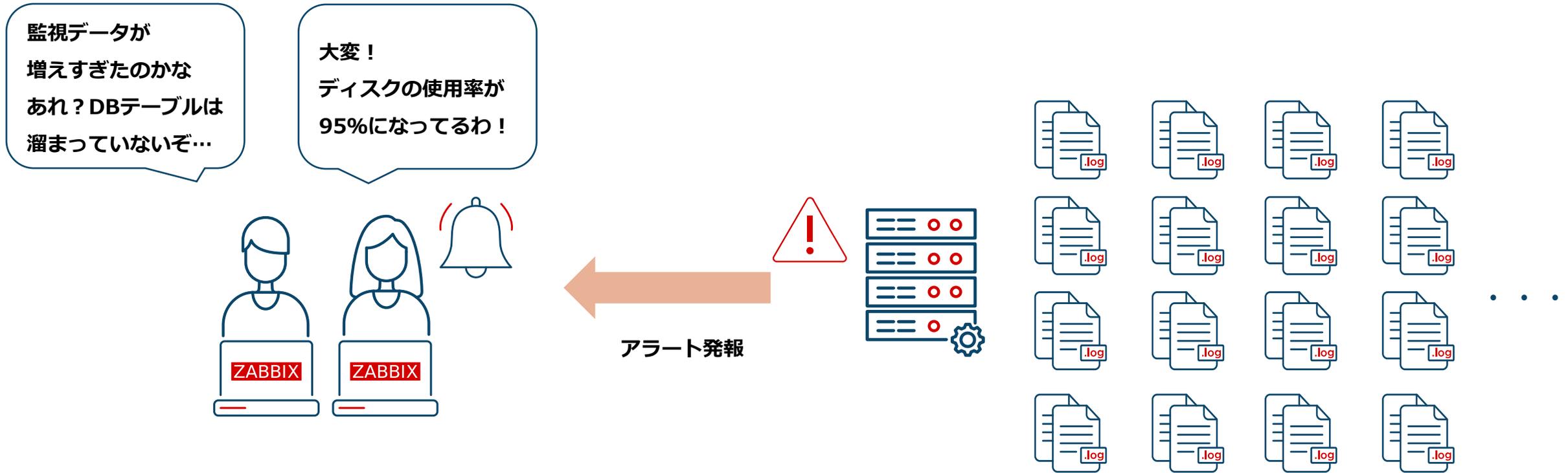
監視の検証や、設定の追加により、RDBのバイナリログがディスクに蓄積

- ▶ バイナリログ…RDB内における、テーブル作成やテーブルデータ変更等の、データベースの内容変更に伴うイベントが書き込まれるログ。



# 課題③ バイナリログによるディスク圧迫

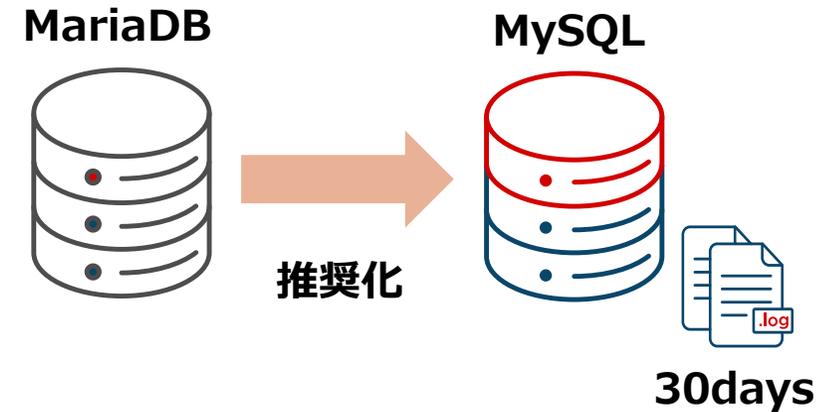
結果、Zabbixサーバのディスクの容量を圧迫し、データを書き込めなくなることも…  
しかし監視データの蓄積が原因でないため、原因特定が難しい。



# 課題③ バイナリログによるディスク圧迫

なぜ起こったのか？

- MariaDBの非推奨化とMySQLの推奨化
- バイナリログの保存ルールの違い
  - MariaDB デフォルトで無効
  - MySQL デフォルトで有効（保存期間30日）



データベースに対する追加・変更・削除が発生すると、バイナリログが生成されるファイルサイズの合計に関わらず、30日分保持してしまう。

- 頻繁な大量ホストへの監視設定投入・修正
- 極端に短い監視間隔の設定

→バイナリログが大量発生してしまう可能性がある。

# 課題③バイナリログによるディスク圧迫

## 解決策

- 暫定対処
  - バイナリログの手動削除（DB内でパージする）
- 恒久対応
  - バイナリログの生成を無効化 → disable-log-bin
  - ローテーション期間を短く設定 → binlog-expire-logs-seconds

コマンド行形式	--binlog-expire-logs-seconds=#
システム変数	<u>binlog_expire_logs_seconds</u>
デフォルト値	2592000（30日）
設定可能範囲	0-4294967295

※expire\_logs\_daysは非推奨

# マイグレーションに伴う運用効率化

# ポート監視除外

## ネットワーク機器の監視に関する要件

- LinkDownが、どのポートで起きたか知りたい
- 表示するポート名を短縮系にしたい
- 特定のポートだけ障害を上げないようにしたい



# ポート監視除外

## ポートごとのLinkDown検知

- SNMPTrapアイテムで、TrapからLinkDownを拾う
  - アイテムタイプ : SNMPTrap
  - アイテムキー : snmptrap[("LinkDown"|"Down"|::LinkDown)]
- 依存アイテムの保存前処理で、受け取ったTrapの中からポートの情報だけを文字列として抽出する

```

SNMP Trap:
Enterprise OID: 1.3.6.1.4.1.9.9.9.1.1.0
Trap Type: LinkDown
Trap OID: IF-MIB::ifDescr.1/0/1
Message: Interface GigabitEthernet 1/0/1 is down
Details:
IF-MIB::ifDescr.1/0/1 type=4 value=STRING: "GigabitEthernet 1/0/1"
  
```

**GigabitEthernet 1/0/1という文字列へ**

保存前処理の設定 ?

名前	パラメータ	失敗時のカスタマイズアクション
1: 正規表現	IF-MIB::ifDescr.\d+\s+type=4\s	<input type="checkbox"/> テスト <input type="checkbox"/> 削除
2: 置換	GigabitEthernet	<input type="checkbox"/> テスト <input type="checkbox"/> 削除

# ポート監視除外

## 表示するポート名の短縮化

文字列として抽出されたポート番号を、保存前処理で省略形に置換する

保存前処理 6

名前	パラメータ	失敗時
1: 正規表現	IF-MIB::ifDescr.\d+\s+type=4\s	\1
2: 置換	GigabitEthernet	Gi

**GigabitEthernet 1/0/1 → Gi1/0/1 へ置換**

- WebUI上での視認性の向上
- ホストマクロでの除外設定がしやすい

# ポート監視除外

特定のポートだけアラート上げないようにする

➤ 依存アイテムにトリガーを作成

トリガーキー：

`find(/Template_SNMPTrap_General_v1/linkDown[ifDescr],, "regexp", {$EXCLUSION.PORT})=0`

→`{$EXCLUSION.PORT}`の値に一致しないポートのみを障害とするが…

テンプレート

テンプレート タグ マクロ 1 値のマッピング

テンプレートのマクロ 継承したマクロとテンプレートマクロ

マクロ	値		説明
<code>{\$EXCLUSION.PORT}</code>	("no-pattern")	T v	SAMPLE : (GigabitEthernet0/(15 16 17))

追加

テンプレートマクロには、「絶対に一致しない」値を設定  
→当然、全てのポートのLinkDownが障害となる

# ポート監視除外

特定のポートだけアラート上げないようにする  
ホストマクロ設定

ホスト IPMI タグ マクロ 1 インベントリ ● 暗号化 値のマッピング

ホストマクロ 継承したマクロとホストマクロ

マクロ	値	説明
{\$EXCLUSION.PORT}	Gi1/0/1	T ↓ 説明

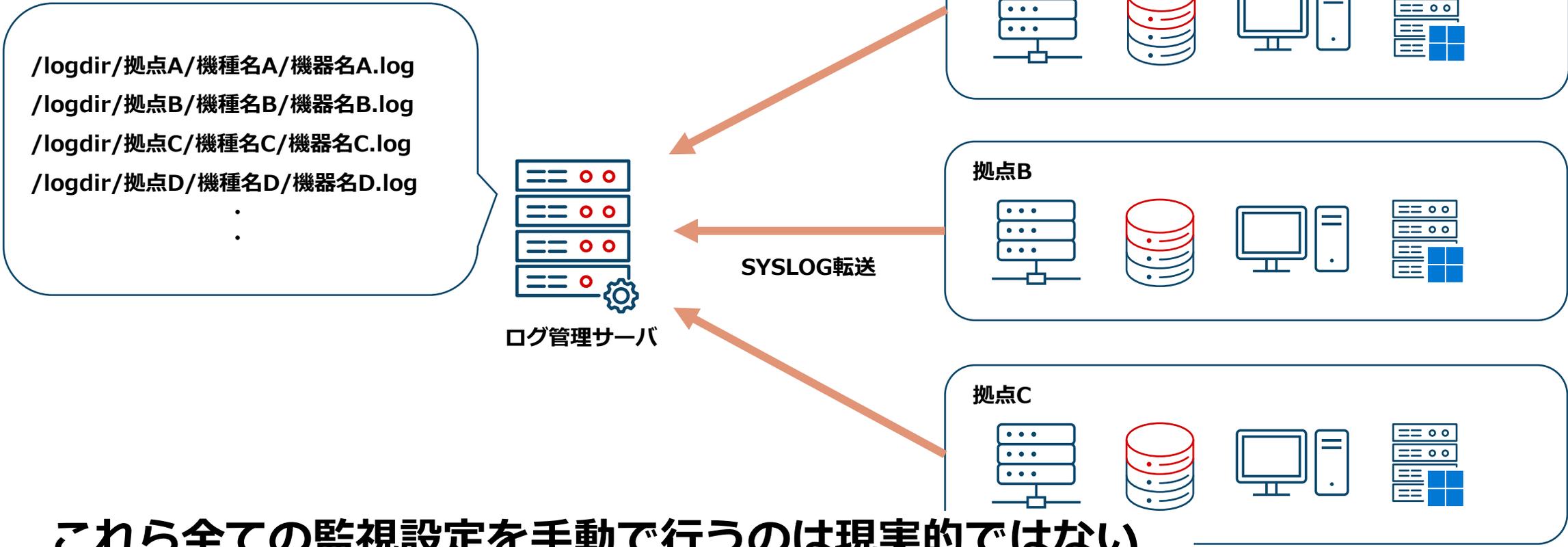
追加

**ホストマクロには、「除外したいポート名」を設定**

- ホストマクロ> テンプレートマクロ
- 除外したいポートだけを、ホストごとに指定できる

# ディスカバリによるログ管理サーバ監視

大規模な環境だと、ログ管理サーバに保存されるSYSLOGの数も膨大となり  
ファイル構造も複雑化する



これら全ての監視設定を手動で行うのは現実的ではない

# ディスクバリによるログ管理サーバ監視

ディスクバリを用いた一括監視設定

使用アイテムキー「vfs.dir.get」 → 対象のディレクトリ情報を取得可能

`vfs.dir.get`[ディレクトリへの絶対パス, 含める文字列, 除外する文字列, 対象とするエントリ種類]

→ `vfs.dir.get` [/logdir/拠点\*, log\$, gz, file]

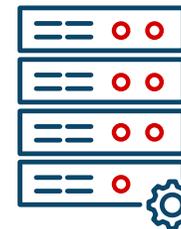
行末が「~log」

同ディレクトリ内の  
圧縮ファイルの除外



Zabbixサーバ

ログファイル  
ディスクバリ



ログ管理サーバ

/logdir/拠点A/機種名A/機器名A.log  
 /logdir/拠点B/機種名B/機器名B.log  
 /logdir/拠点C/機種名C/機器名C.log  
 /logdir/拠点D/機種名D/機器名D.log  
 ⋮  
 ⋮  
 ⋮

# ディスカバリによるログ管理サーバ監視

取得したファイル情報は**JSON形式**であり、そのままでは変数として使用できない  
 →LLDマクロタブの設定で**Zabbix**が**使用できるLLDマクロ**に置き換える

```
[root@Kensyo-ZS7 custom]# zabbix_get -s 127.0.0.1 -p 10050 -k "vfs.dir.get[/var/log/custom,log$,gz,file]" | jq
```

```
{
  "basename": "DeviceName3.log",
  "pathname": "/var/log/custom/AreaName3/DeviceName3.log",
  "dirname": "/var/log/custom/AreaName3",
  "type": "file",
  "user": "root",
  "group": "root",
  "permissions": "rwxr-xr-x",
  "uid": 0,
  "gid": 0,
  "size": 2464,
  "time": {
    "access": "2022-07-27 17:31:15",
    "modify": "2022-07-27 17:25:15",
    "change": "2022-07-27 17:25:15"
  },
  "timestamp": {
    "access": 173115,
    "modify": 172515,
    "change": 172515
  }
}
```

LLDマクロ	JSONPath	
{#BASENAME}	\$.basename	削除
{#PATHNAME}	\$.pathname	削除

追加

更新 複製 テスト 削除 キャンセル

この情報を基に、**アイテムプロトタイプ**を作成

# ディスカバリによるログ管理サーバ監視

## ログ取得アイテムのプロトタイプの作成

アイテムのプロトタイプ タグ1 保存前処理

\* 名前 {#BASENAME} **LLDマクロで定義したログファイル名**

タイプ Zabbixエージェント(アクティブ) ▼

\* キー log[{#PATHNAME},,,,skip] 選択

データ型 ログ **LLDマクロで定義したログファイルパス**

\* 監視間隔 1s

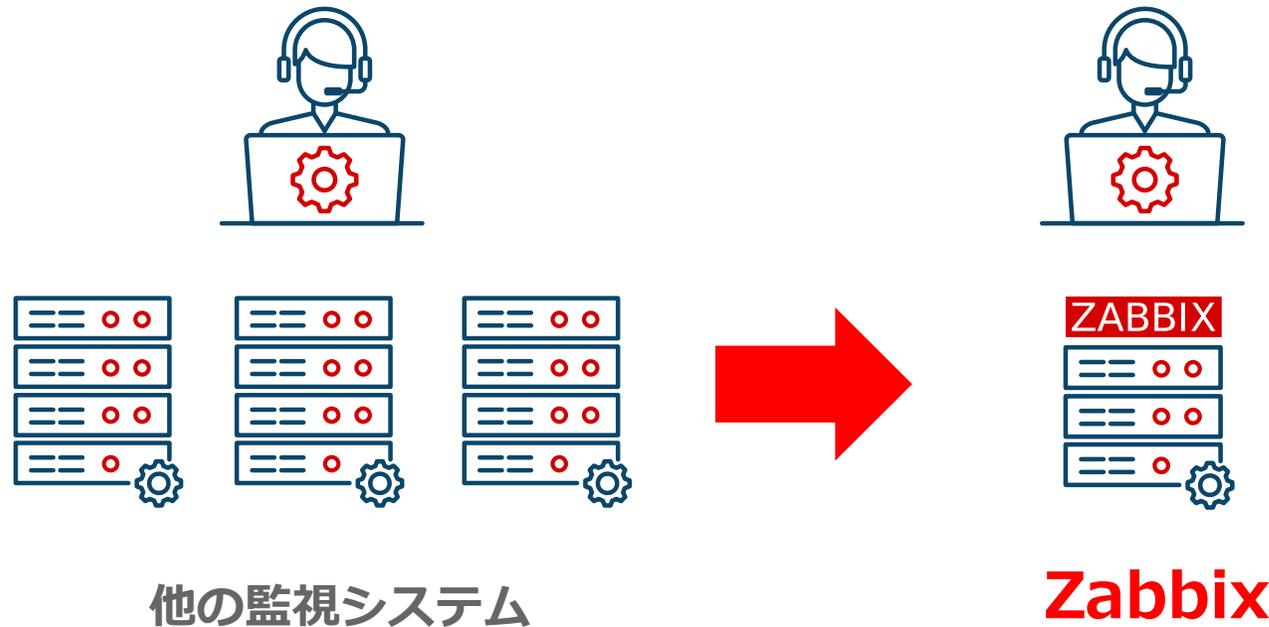
<input type="checkbox"/>	名前	トリガー	キー	監視間隔	ヒストリ
<input type="checkbox"/>	... <b>lldsyslog:</b> DeviceName1.log	<u>トリガー</u> 6	log[/var/log/custom/AreaName1/DeviceName1.log,,,,skip]	1s	31d
<input type="checkbox"/>	... <b>lldsyslog:</b> DeviceName2.log	<u>トリガー</u> 6	log[/var/log/custom/AreaName2/DeviceName2.log,,,,skip]	1s	31d
<input type="checkbox"/>	... <b>lldsyslog:</b> DeviceName3.log	<u>トリガー</u> 6	log[/var/log/custom/AreaName3/DeviceName3.log,,,,skip]	1s	31d

**複雑に階層化されたログファイルのディスカバリを可能に**

# 移行時における注意点

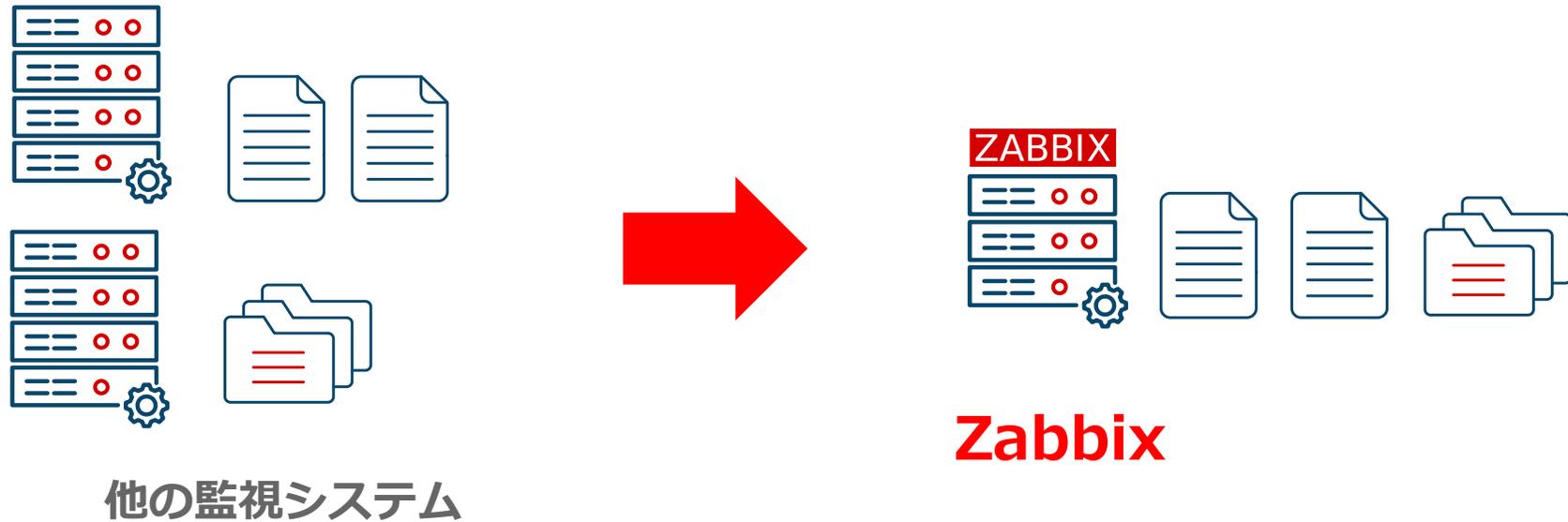
# 移行時における注意点

- 複数システムをZabbixに統合する認識
  - Zabbixを軸とするシステムという認識のもと、他システムをそれに合わせる
  - システム運用者、管理者の強い意志が必要



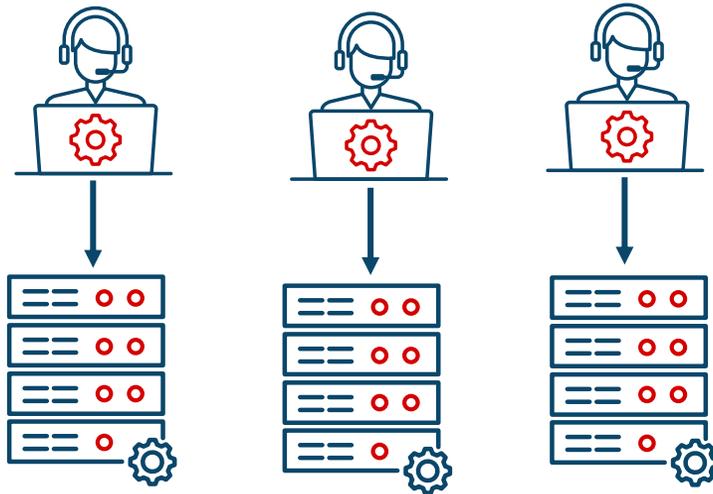
# 移行時における注意点

- Zabbixの仕様に基づいた機能実現の方法
  - やりたいことを言語化し、Zabbixの仕様の範囲内で実現を図る
  - 機能の完全再現は出来ないこともある 出来ないことは諦めも必要

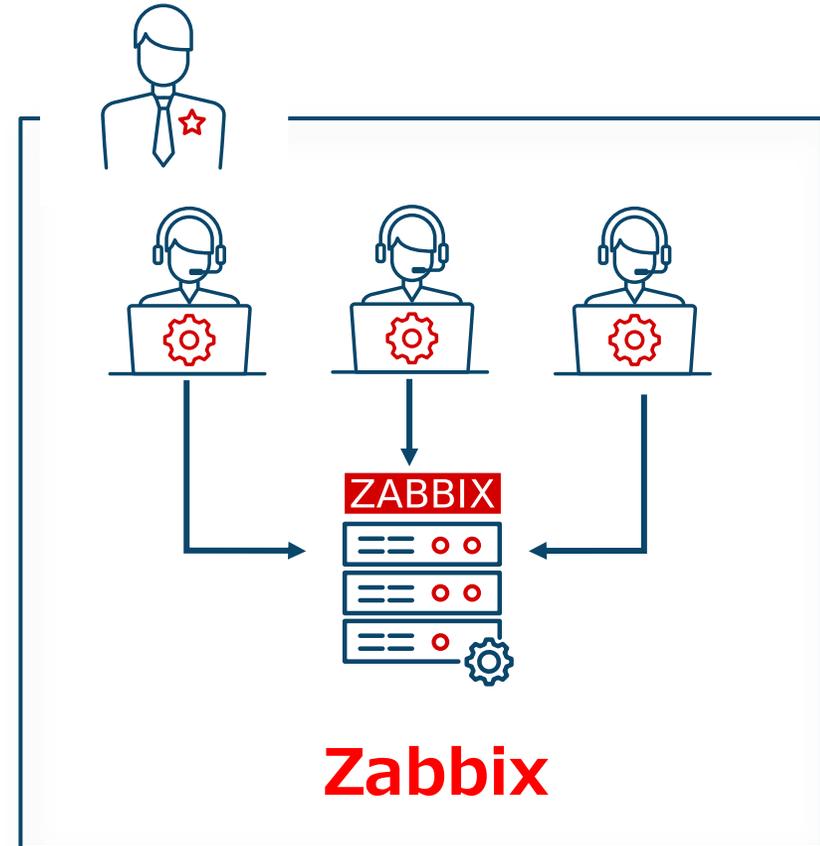
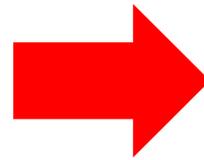


# 移行時における注意点

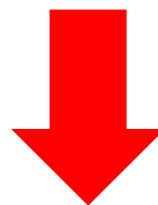
- 業務や体制の柔軟な変更
- システムに合わせた業務や体制の変更
- 柔軟な対応を選択肢に入れる必要性



他の監視システム



マイグレーションは短期的な改善を行うものではない  
現状の課題解決に加え、将来の安定運用や新技術に柔軟に対応できる基盤作り



**Zabbixを通じて  
お客様のシステムの課題解決・安定化を実現する**



**ご清聴ありがとうございました**

# 参考

[https://www.zabbix.com/jp/life\\_cycle\\_and\\_release\\_policy](https://www.zabbix.com/jp/life_cycle_and_release_policy)

<https://www.zabbix.com/documentation/5.0/en/manual/installation/requirements>

<https://www.zabbix.com/documentation/7.0/en/manual/installation/requirements>

<https://dev.mysql.com/doc/refman/8.0/ja/binary-log.html>

[https://mariadb.com/docs/server/ref/mdb/system-variables/max\\_binlog\\_size/](https://mariadb.com/docs/server/ref/mdb/system-variables/max_binlog_size/)