

Zabbix 入門 および Zabbix 最新版 4.2 のご紹介

Zabbix 最新情報セミナー
2019/07/10

SRA OSS, Inc. 日本支社
OSS事業本部 技術部 基盤技術グループ



Zabbix 入門



はじめに

- Zabbix とは
- Zabbix コンポーネント
- アーキテクチャ

Zabbix とは



IT インフラやサービス、アプリケーションの可用性や性能を監視するための
エンタープライズ向け統合監視ソフトウェア



オープンソースソフトウェアとして開発されており、無料で利用可能



開発元はラトビア共和国の Zabbix LLC.



最新バージョンは 4.0（安定版、LTS）と 4.2（ポイントリリース）

Zabbix コンポーネント



Zabbix server

- 全データ収集・保存、障害検知・通知
- Web フロントエンド・データベース含む



Zabbix agent

- ローカル監視データ収集・送信
- パッシブ・アクティブチェック



Zabbix proxy

- 代理でエージェントからのデータを収集
- 負荷分散・集中監視



Zabbix Java gateway

- Java アプリケーション監視用デーモン
- JMX を利用



Zabbix sender

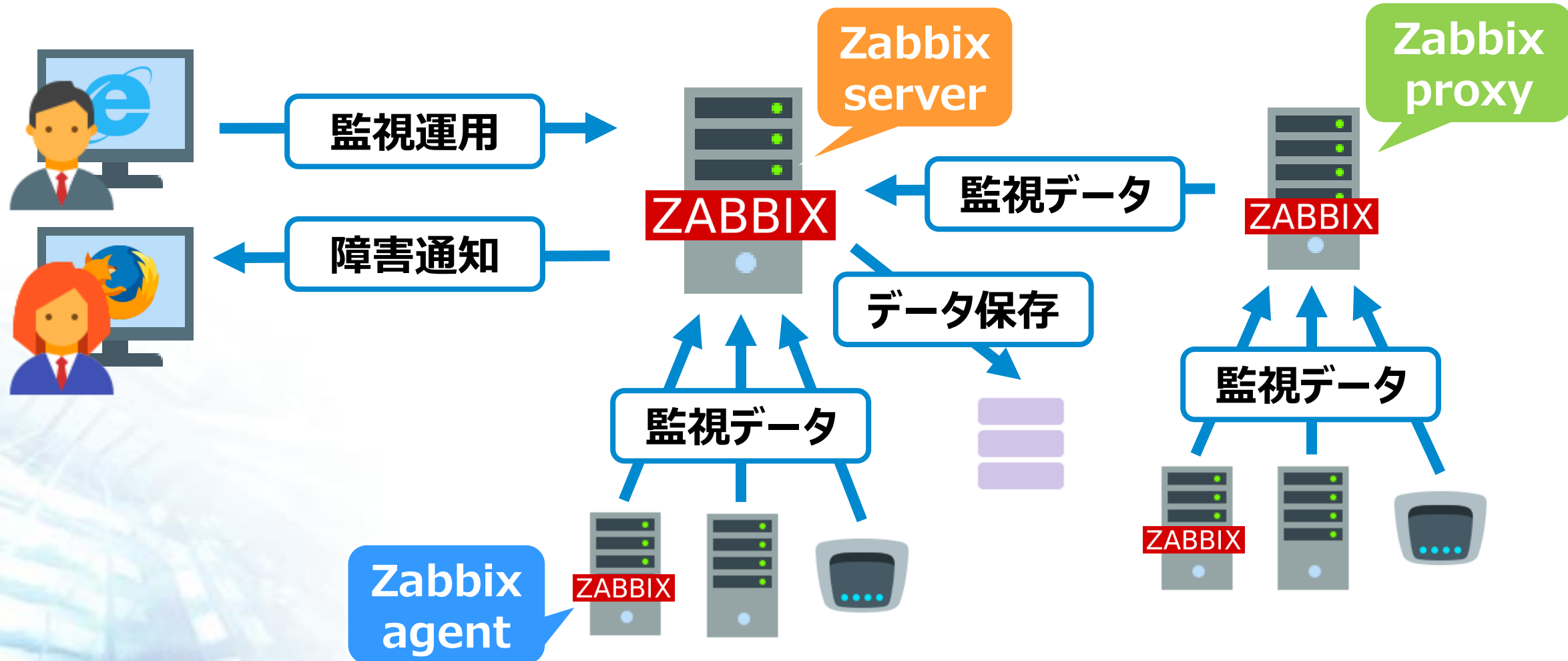
- コマンドラインユーティリティ
- コマンドラインから監視データ送信



Zabbix get

- コマンドラインユーティリティ
- エージェントに特定の監視データを要求

アーキテクチャ

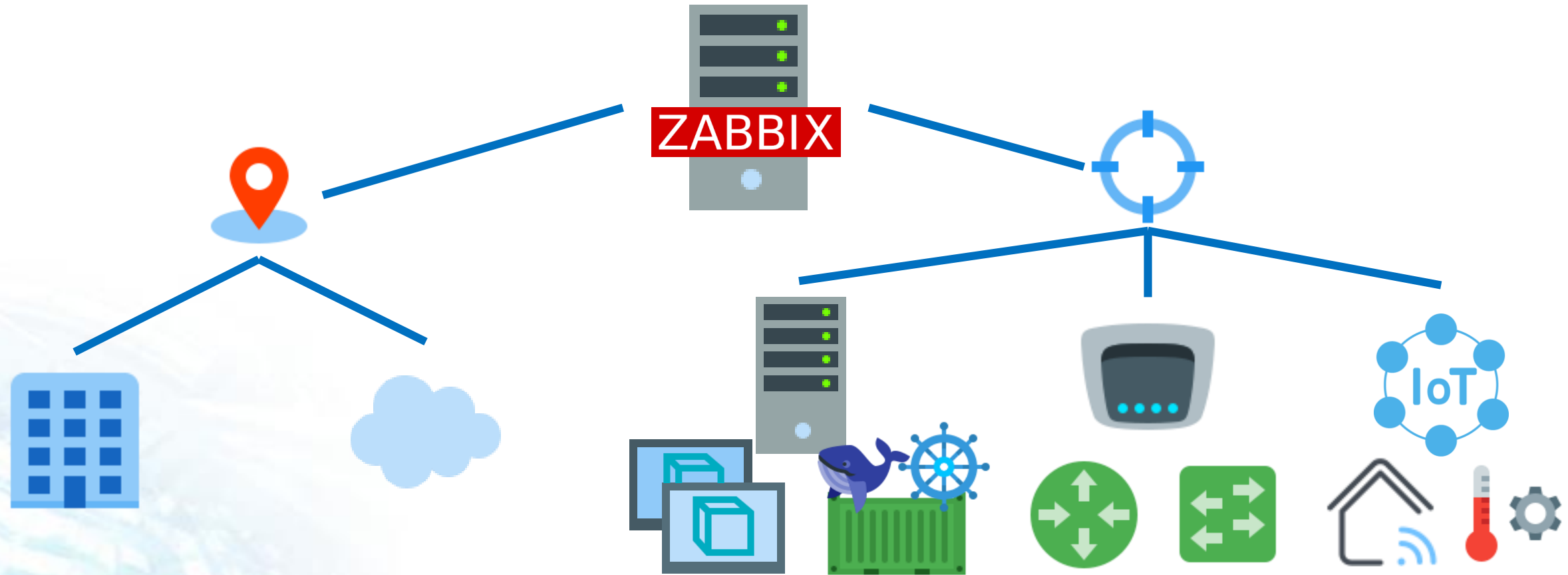




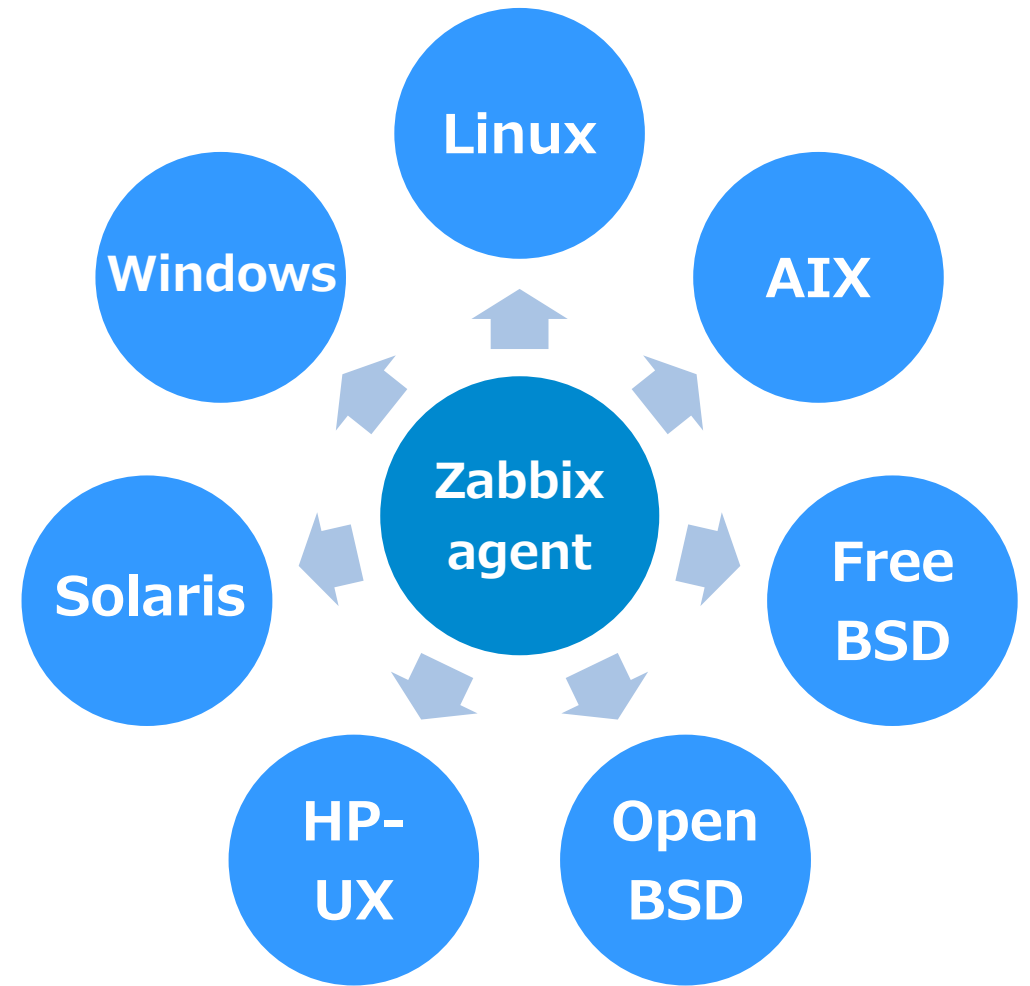
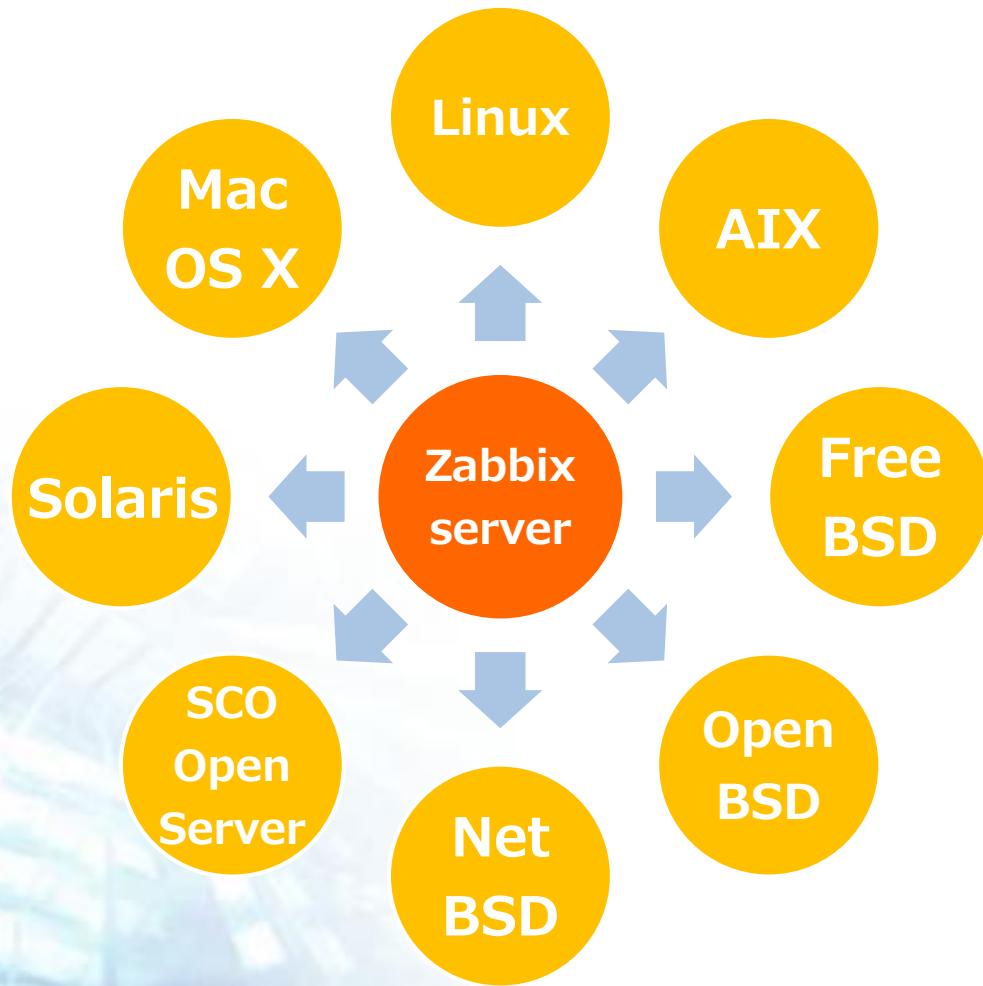
豊富な監視対象

- 監視対象環境
- 対応プラットフォーム
- 監視メトリクス

監視対象環境



対応プラットフォーム

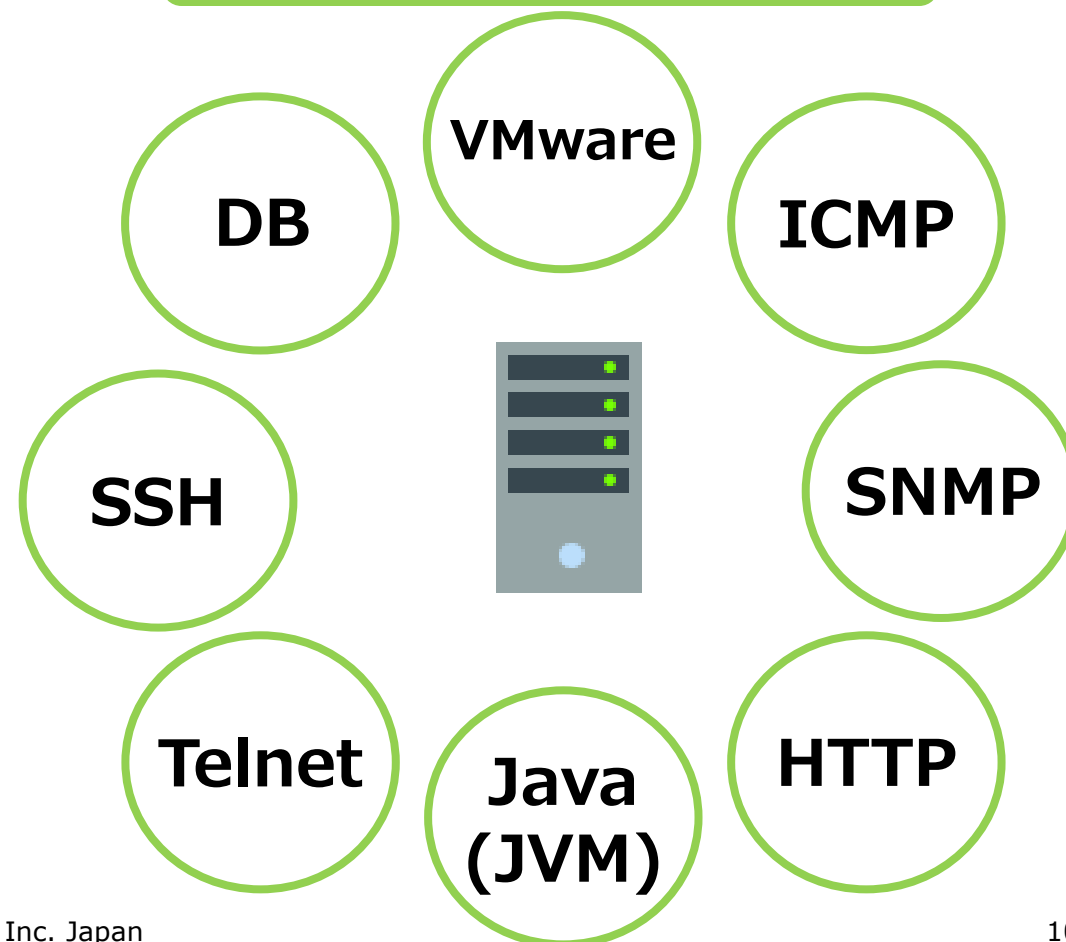


監視メトリクス

エージェント監視



エージェントレス監視

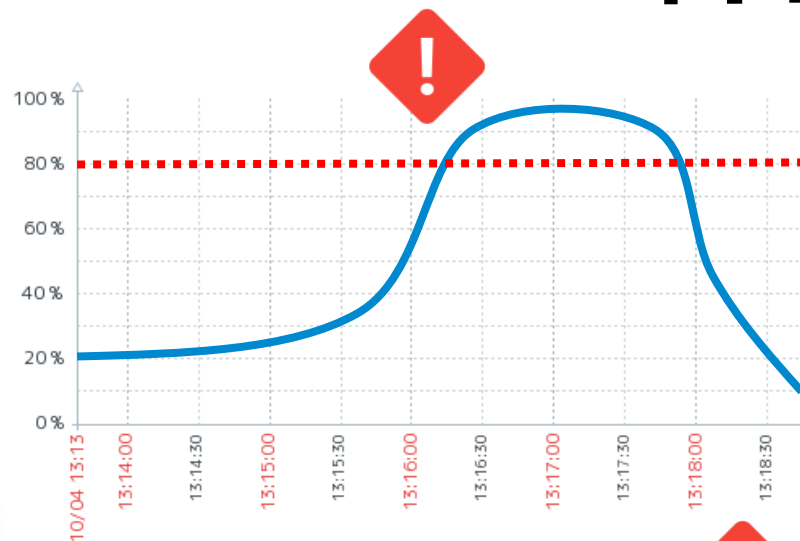




障害検知

障害検知

閾値

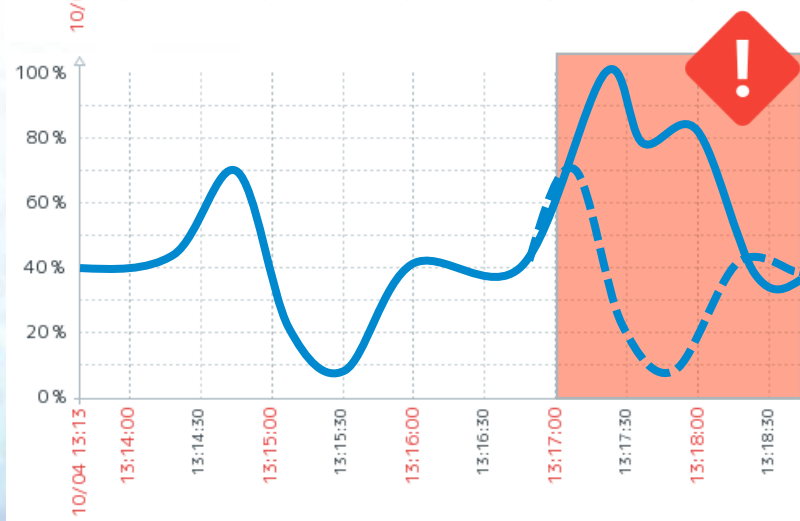


文字列

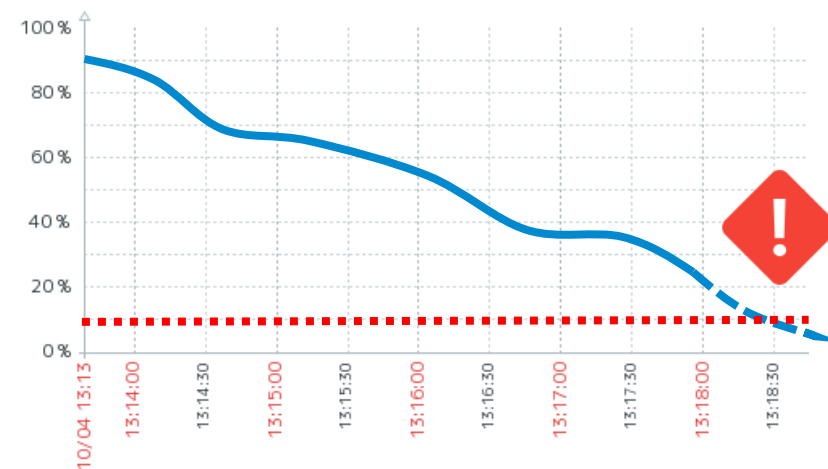
2019 05/14 09:13:25 [INFO] ...
2019 05/14 09:15:10 [ERR] ...
2019 05/14 09:21:47 [INFO] ...



異常値



予測値





障害発生時の通知

- アラート通知とアクション
- エスカレーション

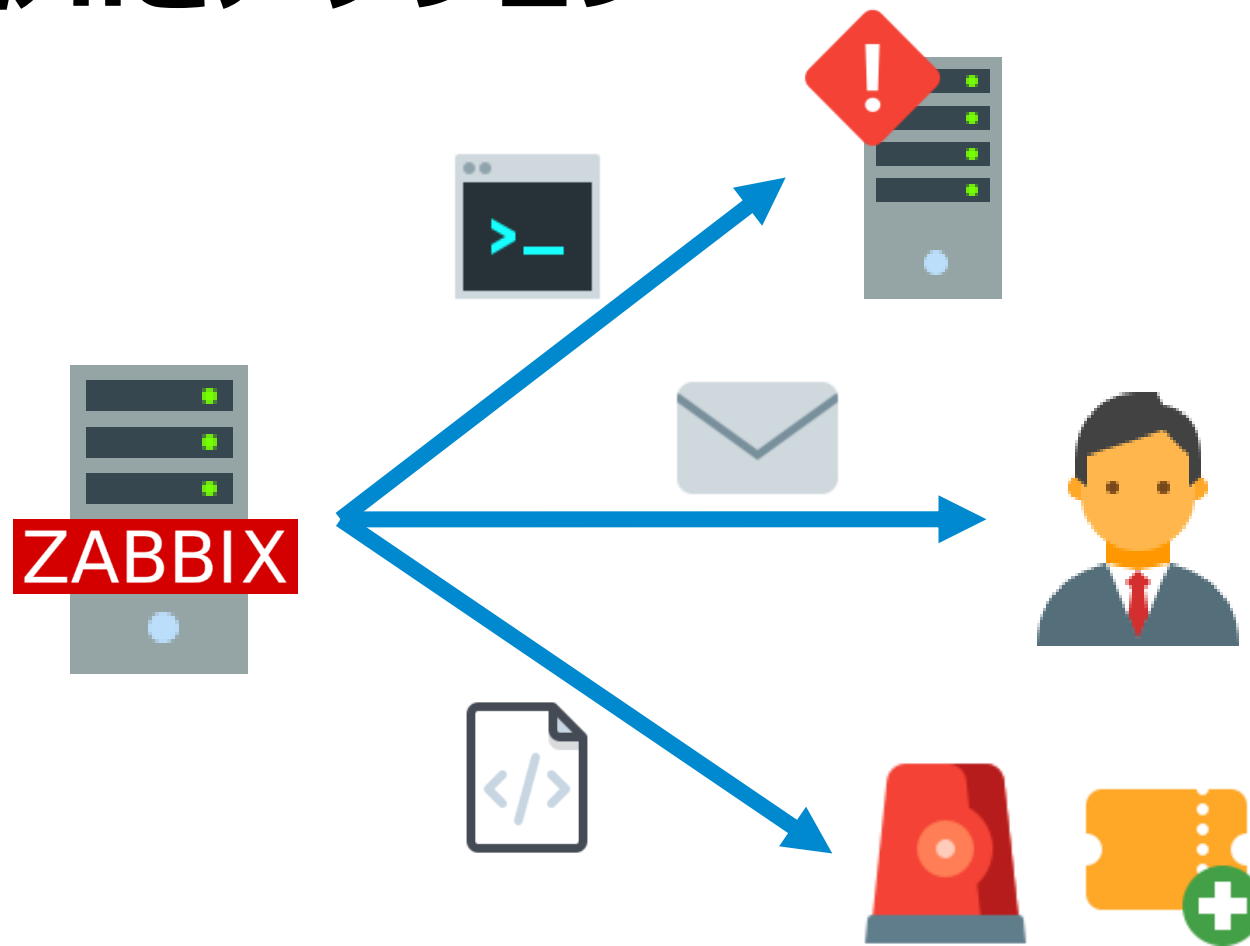
アラート通知とアクション

メッセージ

- E-mail
- SMS
- アラートスクリプト

リモートコマンド

- SSH、Telnet
- IPMI
- カスタムスクリプト



エスカレーション

障害が解消されるまで
段階的に通知を実行

サービス停止

0分後

運用担当にメール

5分後

管理担当にメール

運用担当に再度メール

10分後

サービスの再起動



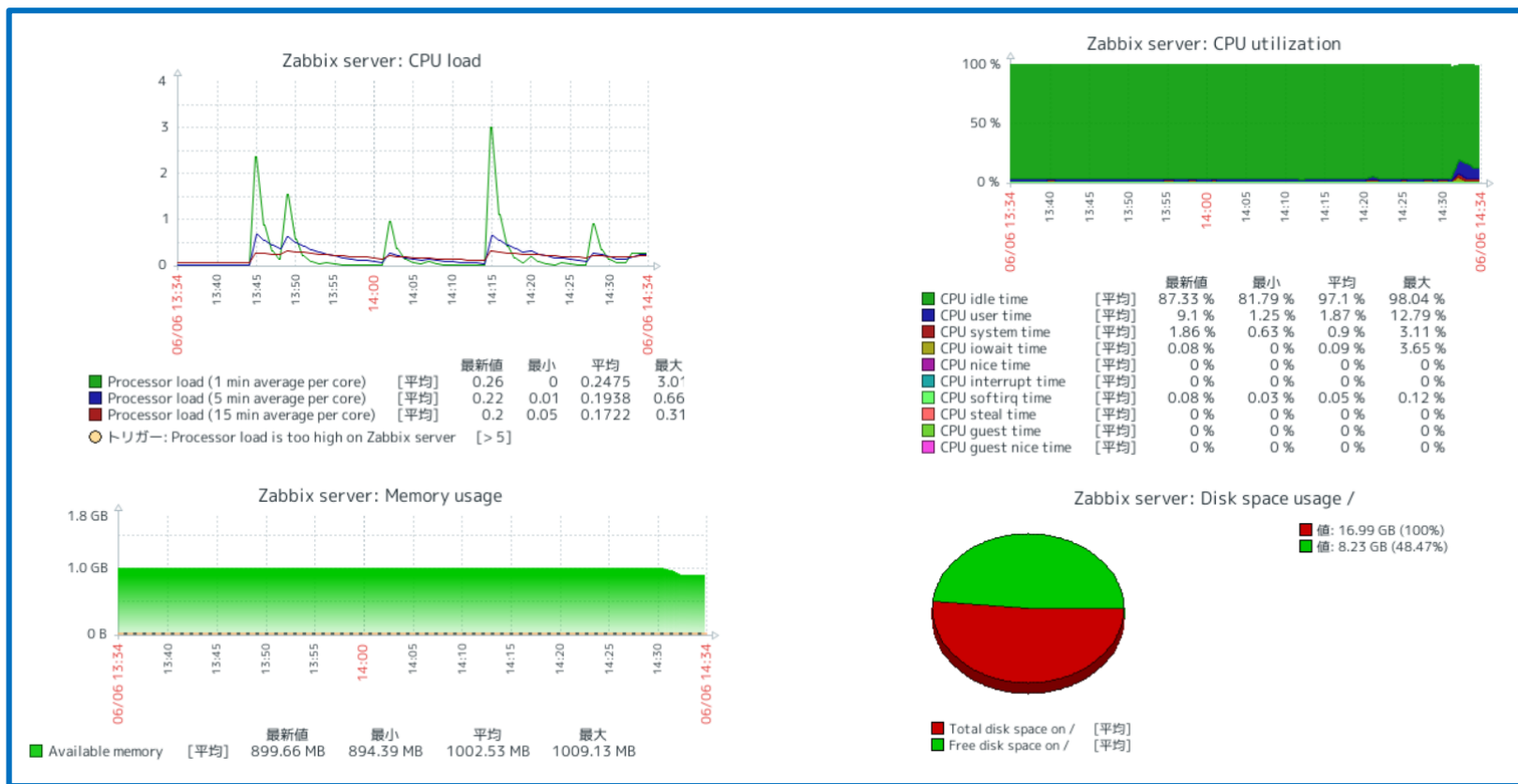
ビジュアライゼーション

- グラフ
- ネットワークマップ
- ダッシュボード

グラフ

収集したデータをグラフ化

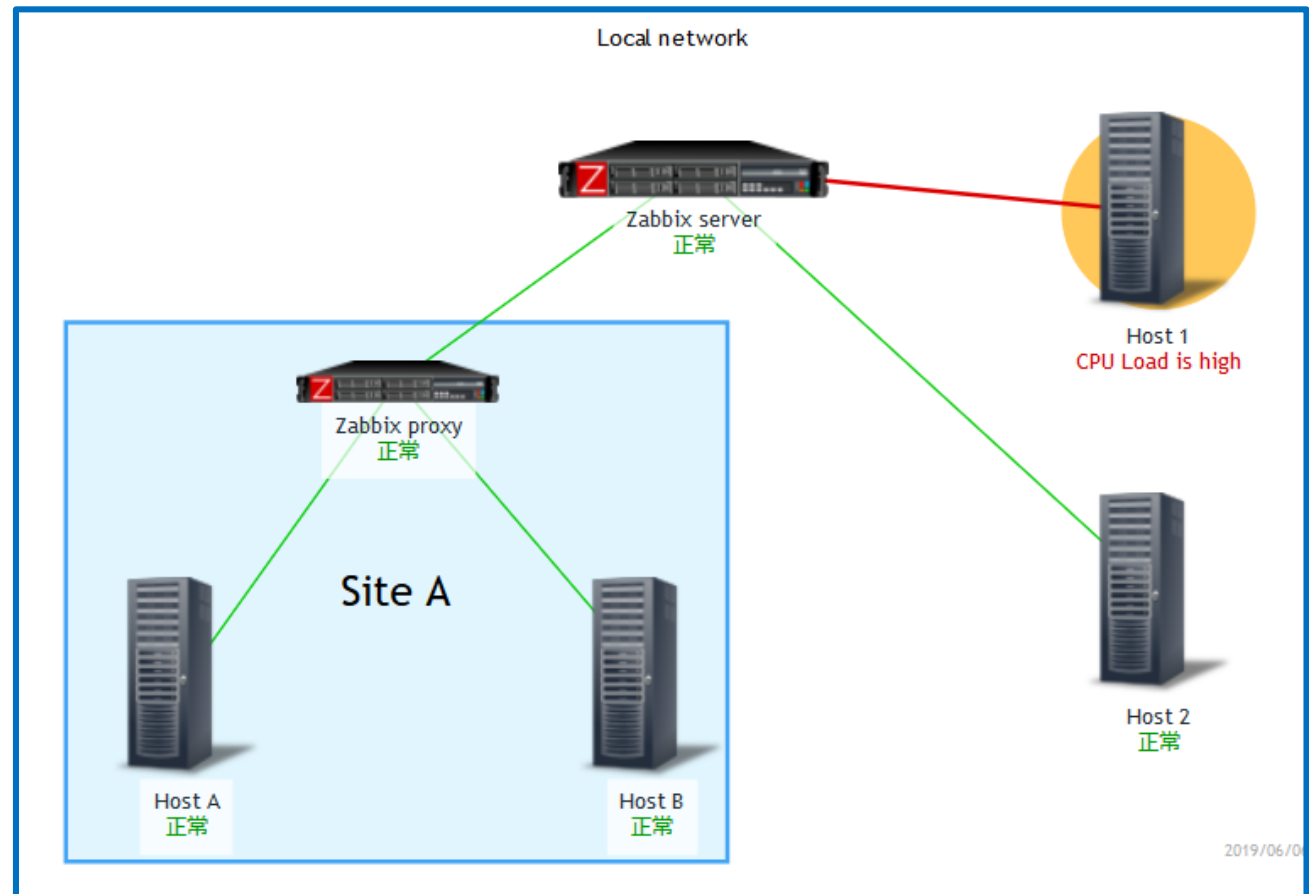
- グラフタイプ
 - 線グラフ
 - 積算グラフ
 - 円グラフ
- 同一グラフ上に複数メトリクス
- 自動更新



ネットワークマップ

監視環境を可視化

- マップ要素
- ホスト
- ホストグループ
- マップ
- 画像
- 障害をマップ上に表示
- 自動更新



ダッシュボード

監視環境を一画面に集約

- 多種のウィジェット
- システムステータス
- 障害情報
- グラフ
- etc.
- ユーザがカスタマイズ可能
- 自動更新





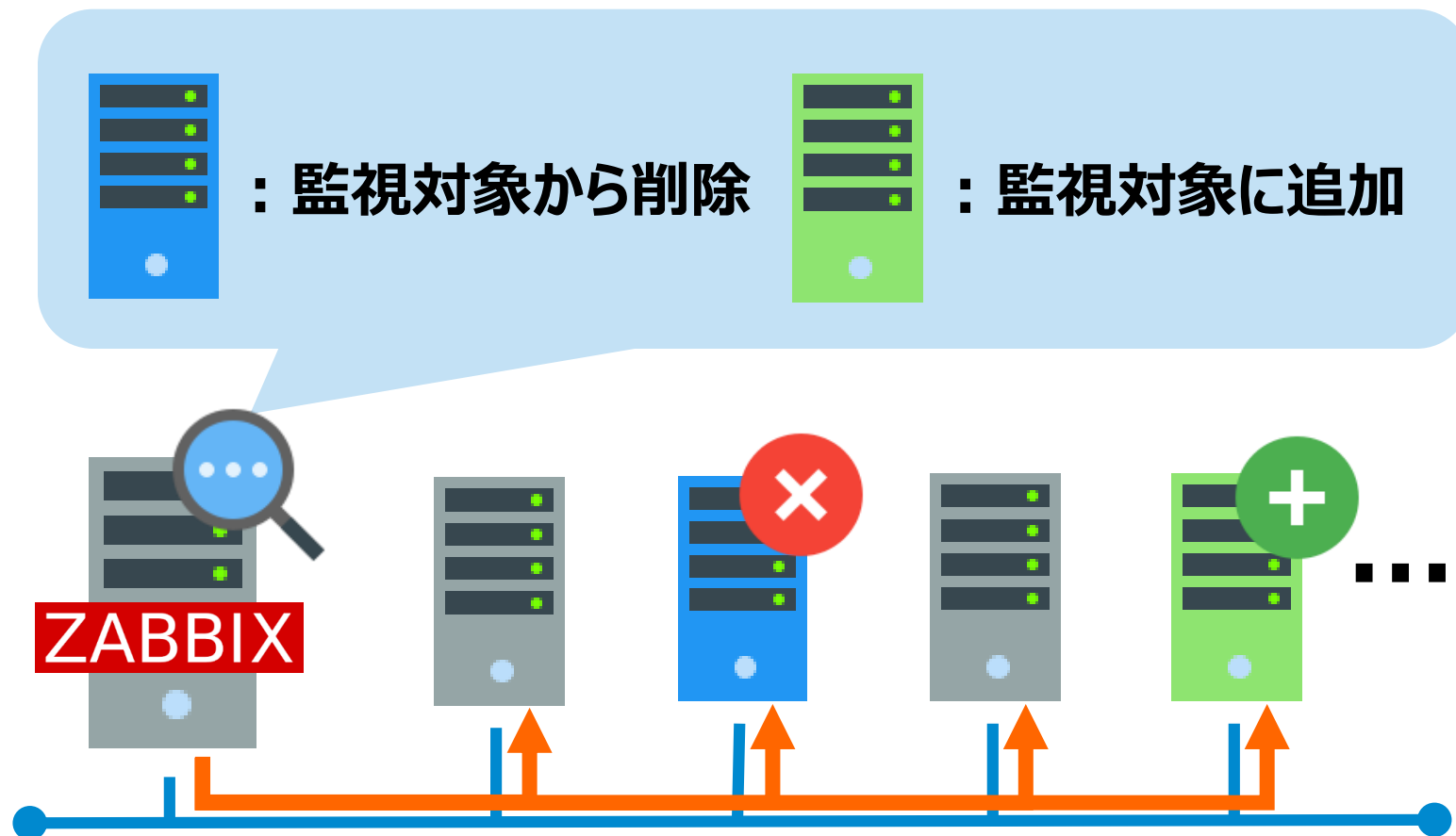
オートディスカバリ

- ネットワークディスカバリ
- アクティブエージェントの自動登録
- ローレベルディスカバリ

ネットワークディスカバリ

ネットワークを探索し
自動でアクションを実行

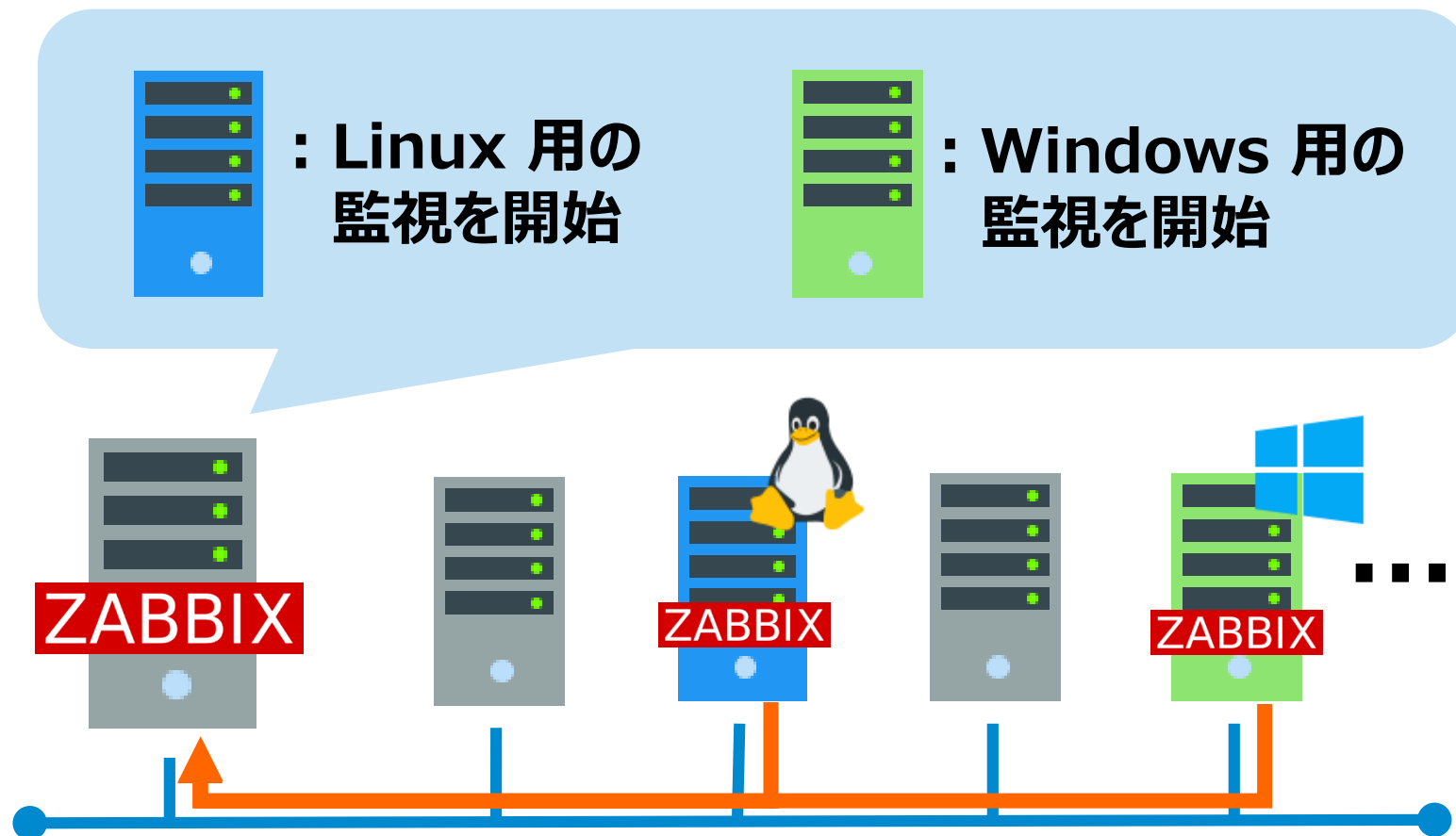
- 探索対象
 - IP アドレス
 - サービス (FTP、SSH、HTTP、SNMP、etc.)
 - Zabbix agent
- アクション
 - 監視対象の追加・削除
 - メトリクスの追加・削除
 - スクリプトの実行



アクティブエージェントの自動登録

Zabbix agent からの 情報により監視を開始

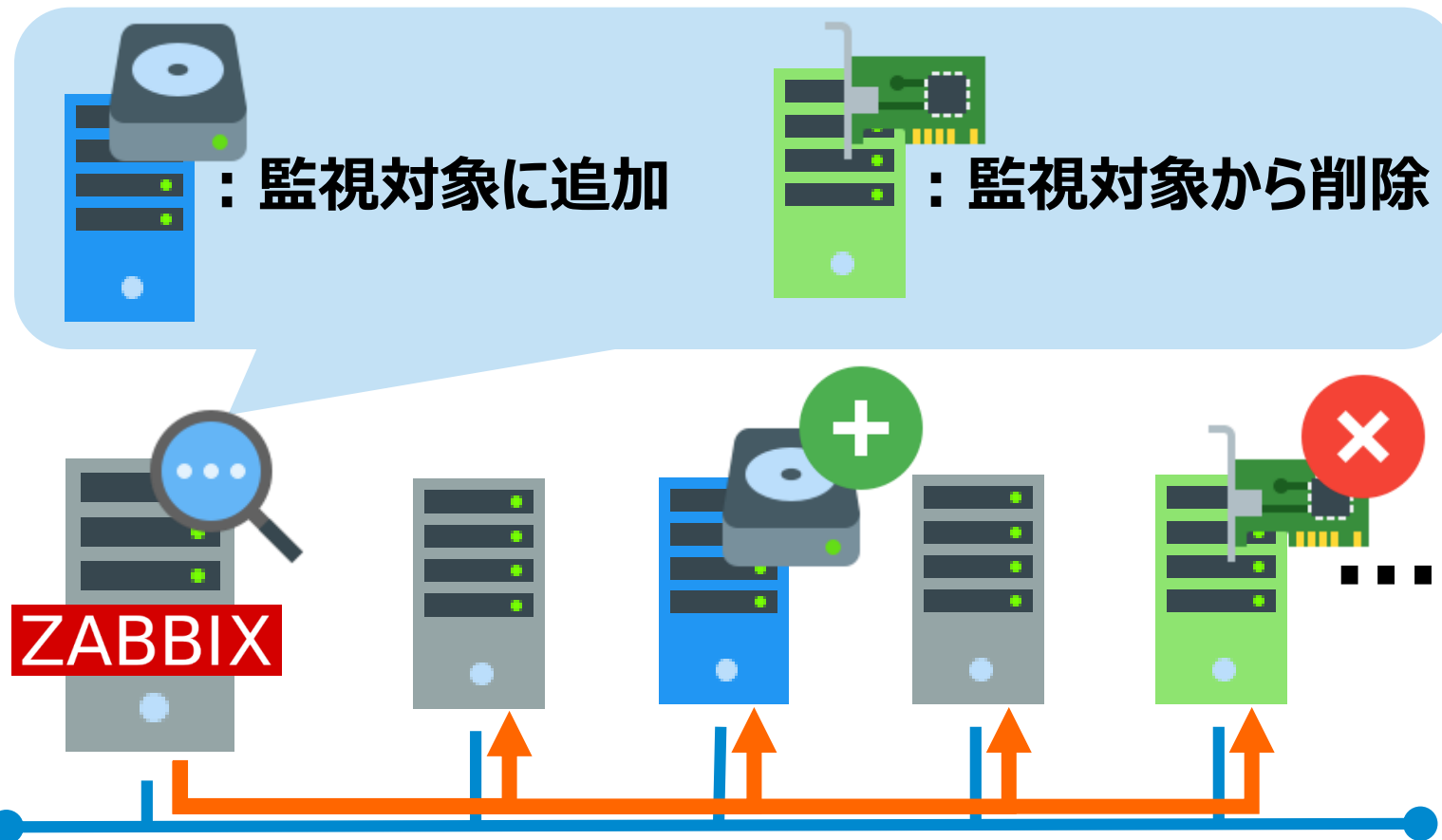
- 監視対象の追加・削除
- メトリクスの追加・削除
- スクリプトの実行
- 通知の送信

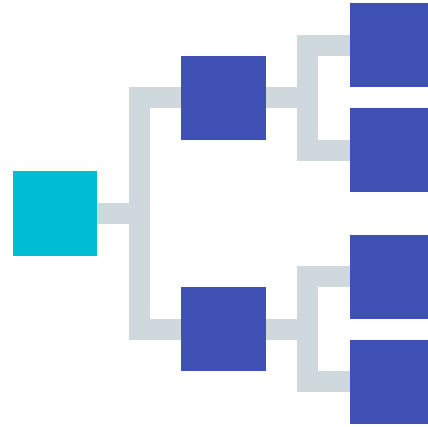


ローレベルディスクカバリ

発見されたデバイスに対して
自動的に監視を開始

- CPU
- ファイルシステム
- ネットワークインタフェース
- SNMP OID
- Windows サービス





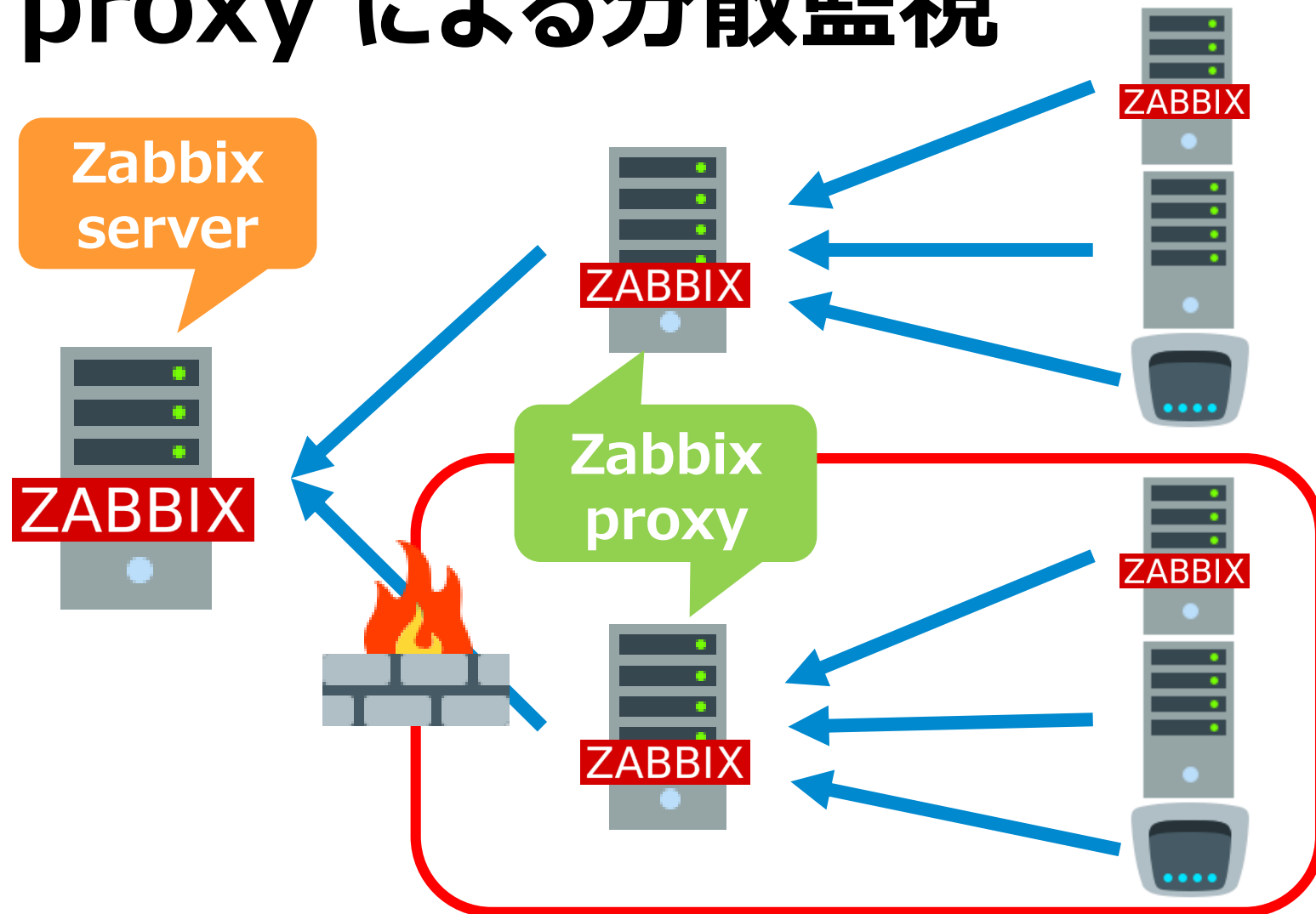
分散監視

- Zabbix proxy による分散監視

Zabbix proxy による分散監視

Zabbix proxy による 集中管理と分散監視

- Zabbix server の
負荷分散
- Firewall や DMZ
越しの監視





セキュリティ

- ユーザ権限
- ユーザグループとパーミッション
- 暗号化通信

ユーザ権限

ユーザ種別	監視結果	監視設定	管理機能
Zabbix ユーザ	✓	✗	✗
Zabbix 管理者	✓	✓	✗
Zabbix 特権管理者	✓	✓	✓

ユーザごとに操作範囲を決定

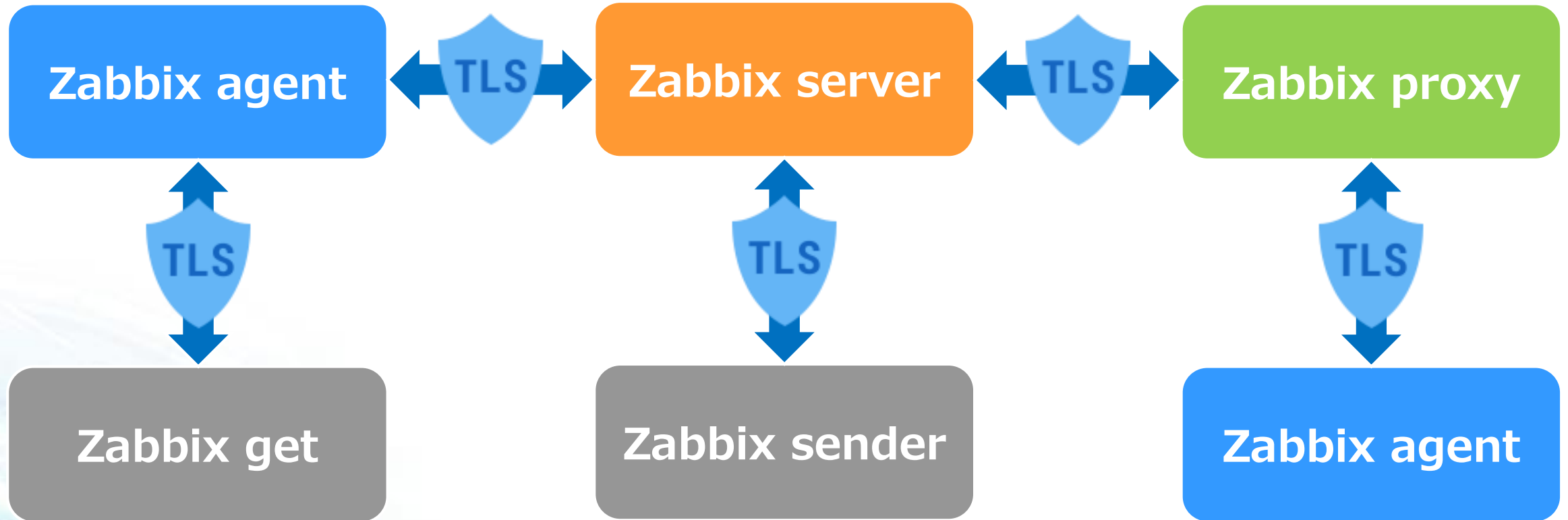
ユーザグループとパーミッション

ユーザグループごとの パーミッション

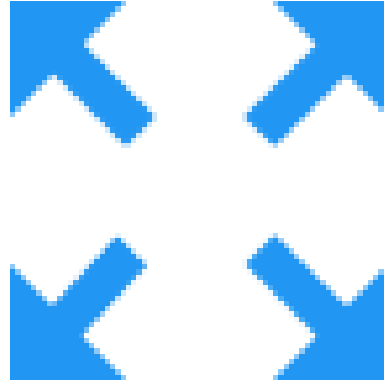
- Read/Write
- Read only
- Deny

暗号化通信



暗号化なし・PSK(事前共有鍵)・証明書を選択可



機能拡張

- Zabbix agent の機能拡張
- Zabbix API

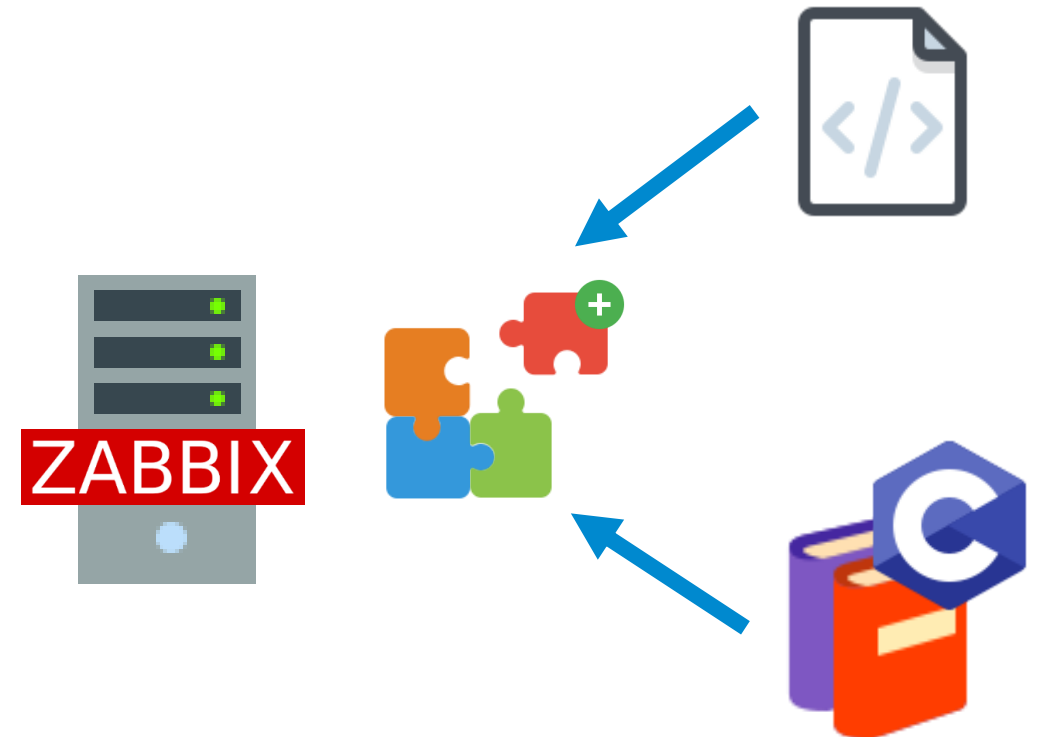
Zabbix agent の機能拡張

ユーザパラメータ

- ユーザ独自のスクリプトによる監視項目を追加

ロードブルモジュール

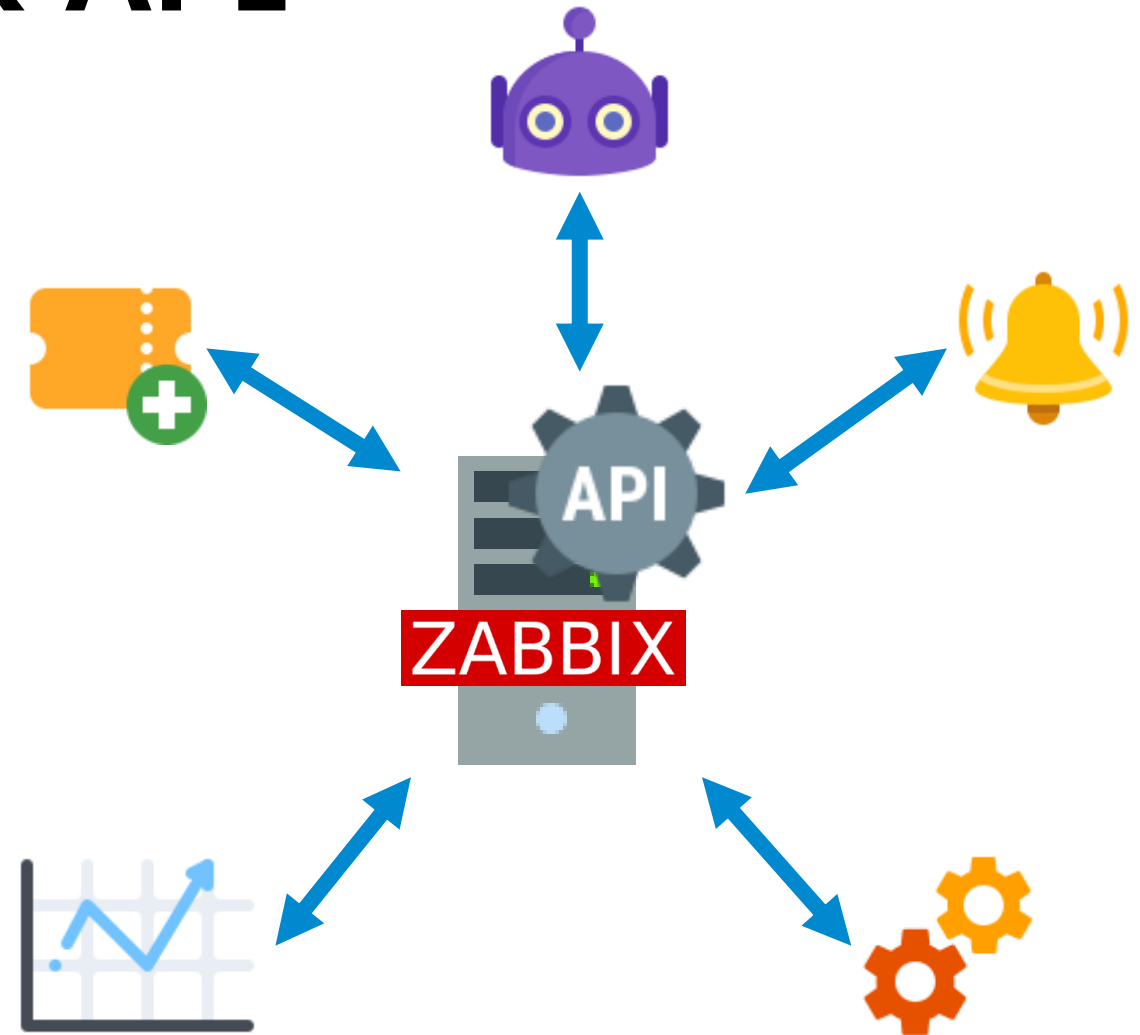
- ユーザ独自の共有ライブラリによる監視項目を追加



Zabbix API

API 経由で Zabbix を操作

- Zabbix のほとんどの機能をカバー
 - 監視設定の追加・変更・削除・参照
 - 収集した監視データの参照
- 外部アプリケーションとの連携
- 独自のアプリケーション作成



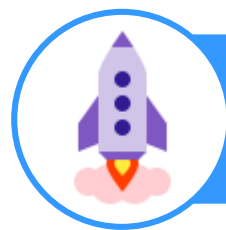
Zabbix 4.2 のご紹介



Zabbix 4.2 について

- Zabbix 4.2 の基本情報
- Zabbix 4.2 の新機能概要

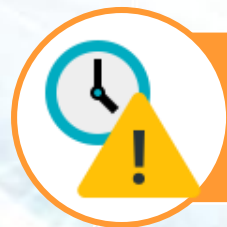
Zabbix 4.2 の基本情報



2019/04/02 : Zabbix 4.2.0 リリース



LTS (Long Term Support) ではなくポイントリリース



2019/09/30 : フルサポート終了
2019/10/31 : リミテッドサポート終了



最新マイナーバージョンは 4.2.4 (2019/07/10 現在)

Zabbix 4.2 の新機能概要

新しく
サポートされる
プラットフォーム

保存前処理の
機能拡張

TimescaleDB
サポート

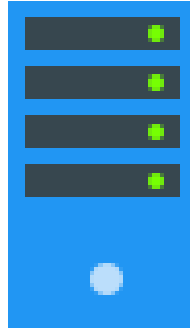
ディスクバリの
機能拡張

Prometheus
との統合

通知・メディアの
機能拡張

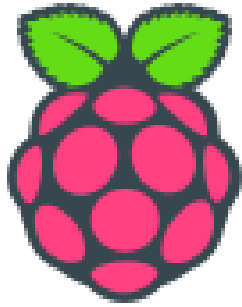
マップの
機能拡張

フロントエンドの
機能拡張



新しくサポートされる プラットフォーム

新しくサポートされるプラットフォーム



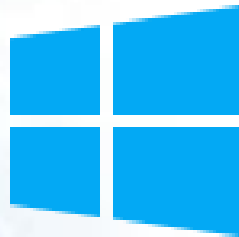
RaspberryPi



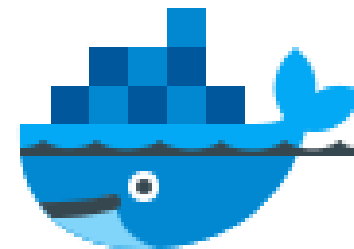
Mac OS/X



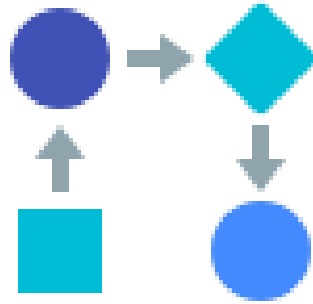
**SUSE Enterprise
Linux Server 12**



Windows エージェントの MSI



Docker イメージ



保存前処理の機能拡張

- JavaScript
- バリデーションと絞り込み
- 失敗時のカスタマイズ
- 保存前処理のテスト
- Zabbix proxy でのサポート
- エラーメッセージの拡張

保存前処理の復習



取得したデータを加工して保存

JavaScript

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: JavaScript	スクリプト	☐	テスト 削除

追加

更新 複製 監視データ取得 削除

パラメータに
スクリプトを直接入力

JavaScript

```
function (value) {  
  1 var databases = [];  
  2 var lines = value.split('\n');  
  3  
  4 databases = lines.slice(2,-1).map(function(value, index) {  
  5     var ret = {};  
  6     ret['{#DATABASE}'] = value.replace(/ /g, '');  
  7     return ret;  
  8 });  
  9  
 10 return JSON.stringify(databases);  
}
```

JavaScript



バリデーションと絞り込み

- 値の範囲
- 正規表現と一致する/しない
- JSON内/XML内/正規表現
使用時のエラーチェック

バリデーション



- 変化がなければ破棄
- 指定秒内に変化がなければ
破棄

絞り込み

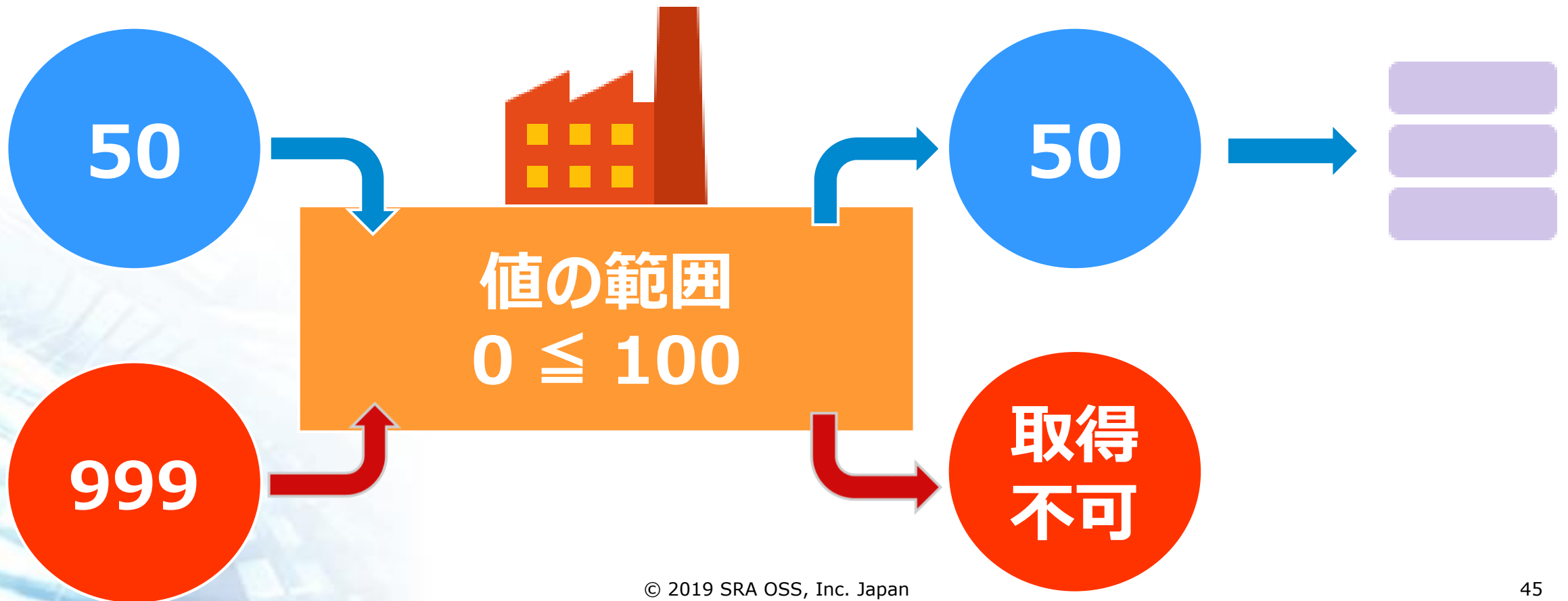


バリデーション － 値の範囲 －

アイテム	保存前処理	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:	値の範囲	最小	最大	☐	テスト 削除

取得した値が想定の範囲内かどうかを確認

バリデーション － 値の範囲 －



バリデーション

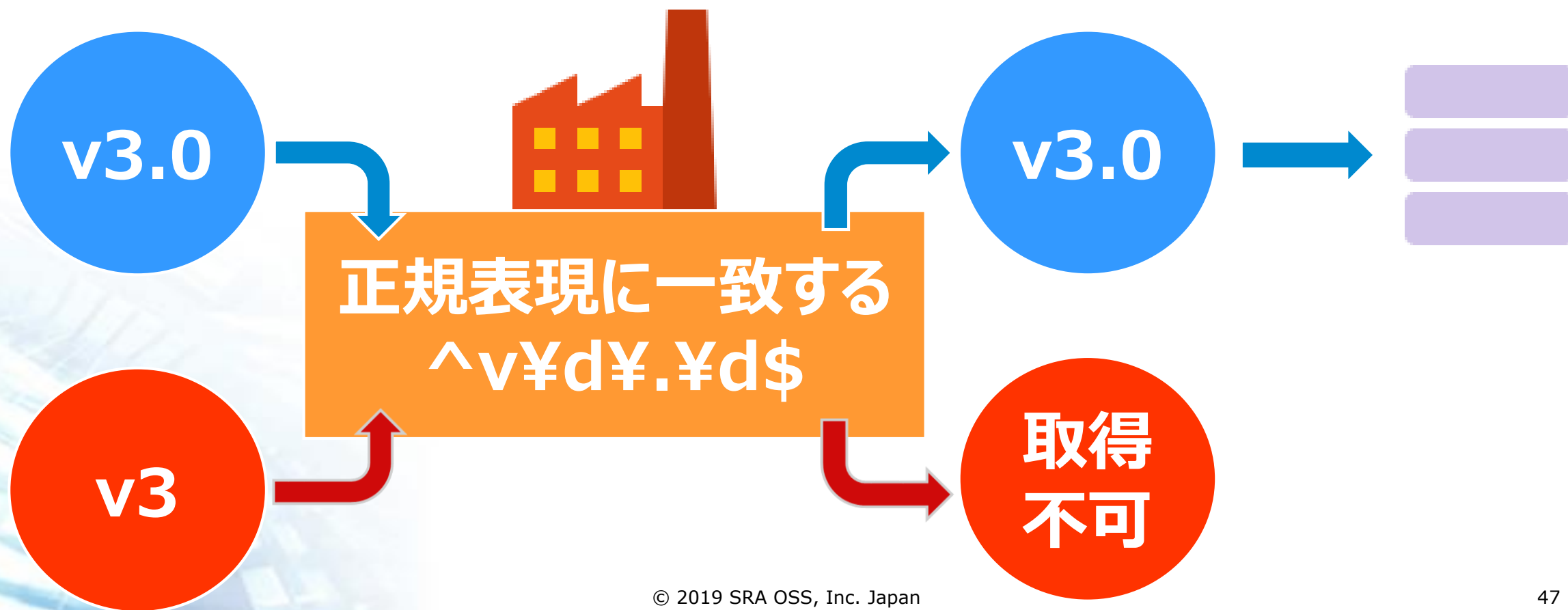
－ 正規表現に一致する/しない－

アイテム		保存前処理			
		保存前処理の設定		失敗時のカスタマイズ	アクション
		名前	パラメータ		
1:	正規表現と一致する	▼	パターン	☐	テスト 削除
	2: 正規表現と一致しない	▼	パターン	☐	テスト 削除

取得した値が正規表現に一致する/しないを確認

バリデーション

– 正規表現に一致する/しない –



バリデーション

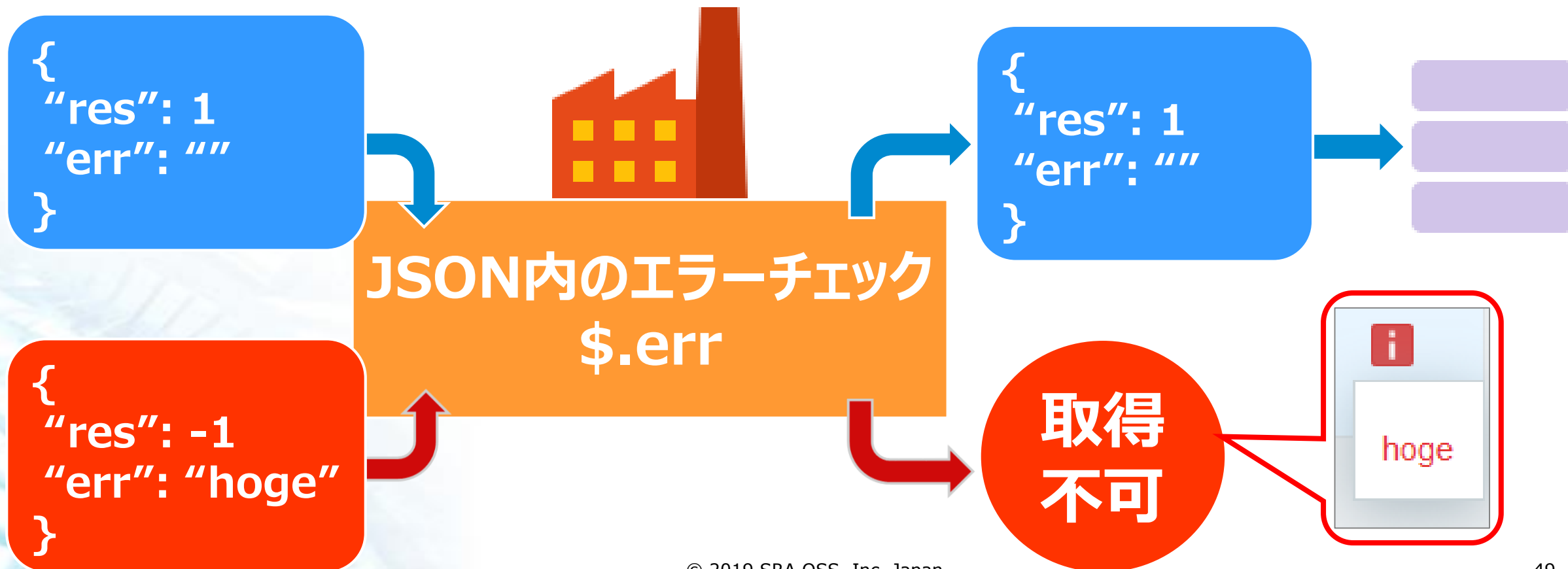
– JSON内/XML内/正規表現使用時のエラーチェック–

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:	JSON内のエラーチェック	▼	\$path.to.node	☐	テスト 削除
2:	XML内のエラーチェック	▼	XPath	☐	テスト 削除
3:	正規表現使用時のエラーチェック	▼	パターン	☐	テスト 削除
			出力		

取得した値にエラーメッセージが含まれるか確認

バリデーション

– JSON内/XML内/正規表現使用時のエラーチェック–

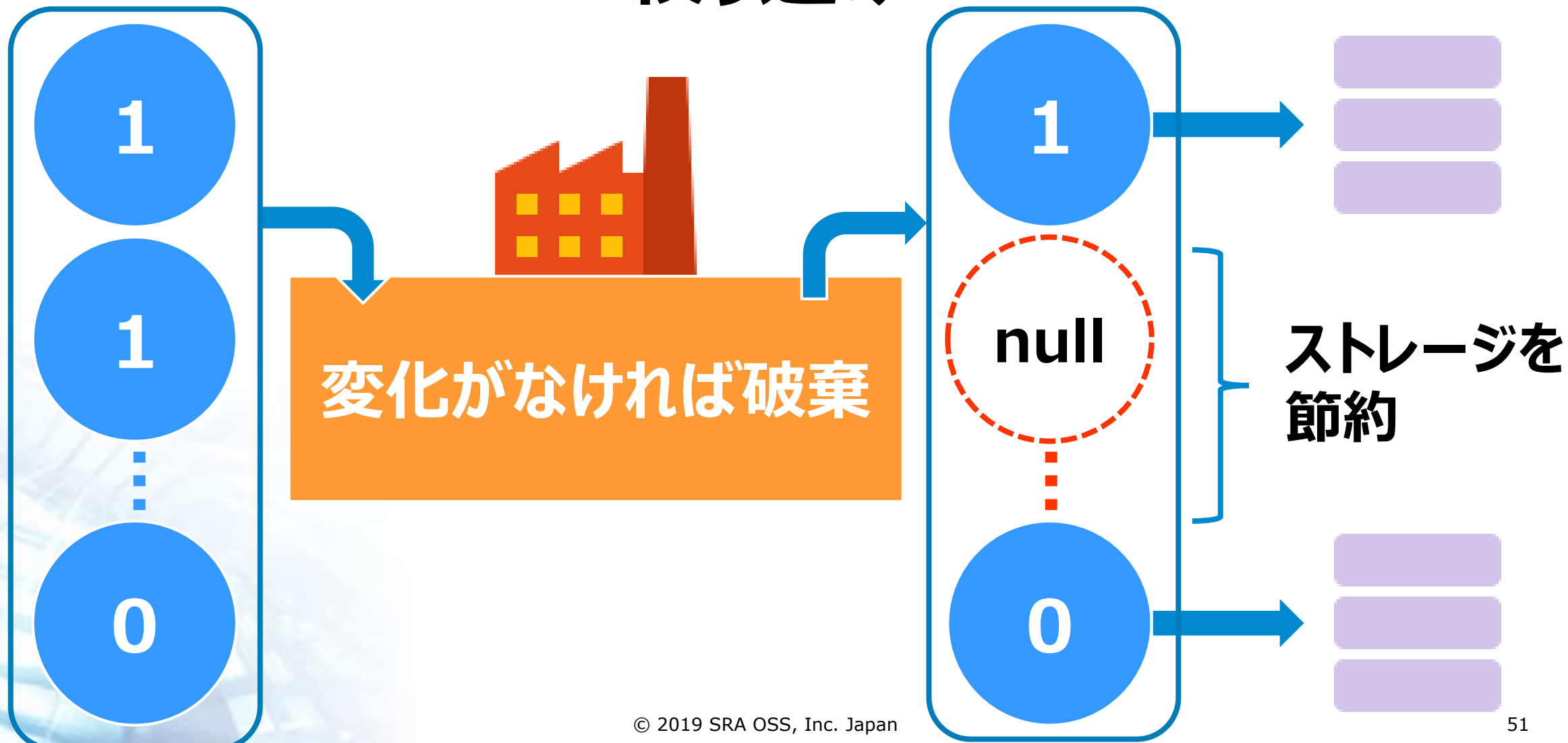


絞り込み

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:	変化がなければ破棄	▼	☐	テスト 削除
⋮ 2:	指定秒内に変化がなければ破棄	▼ 秒	☐	テスト 削除

取得した値に変化があれば保存、なければ破棄

絞り込み

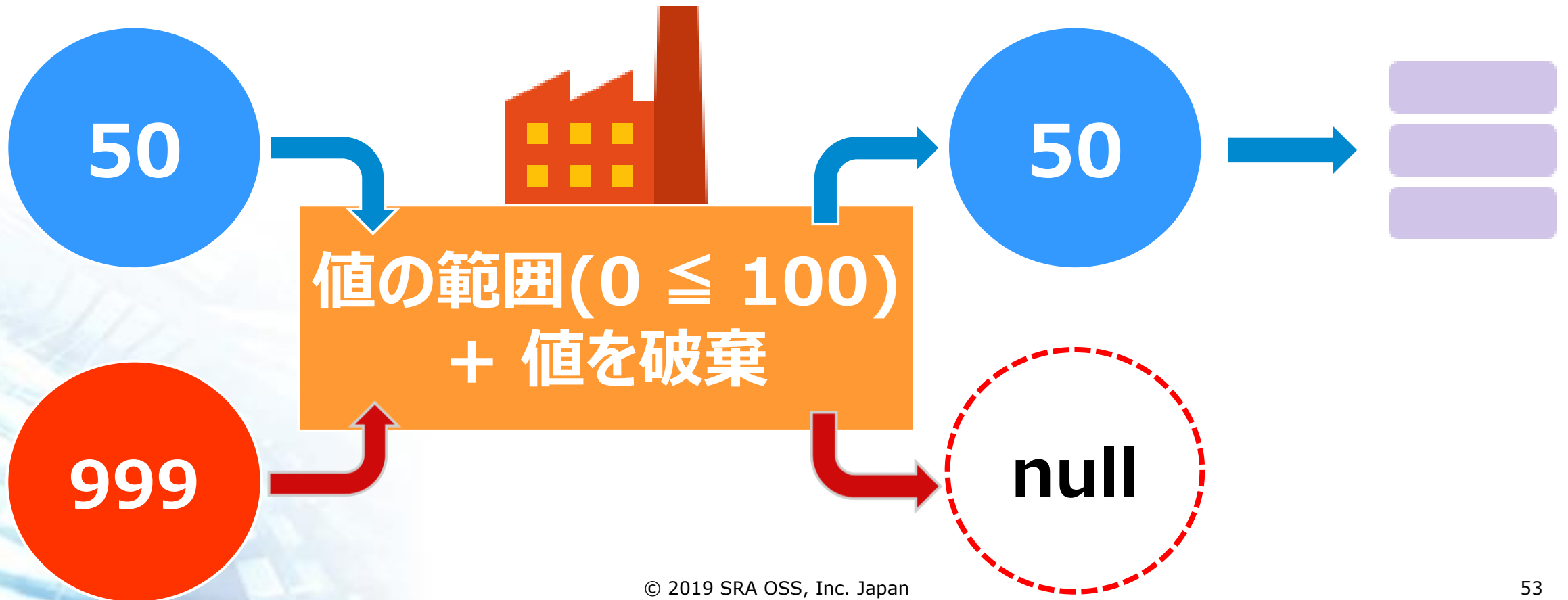


失敗時のカスタマイズ

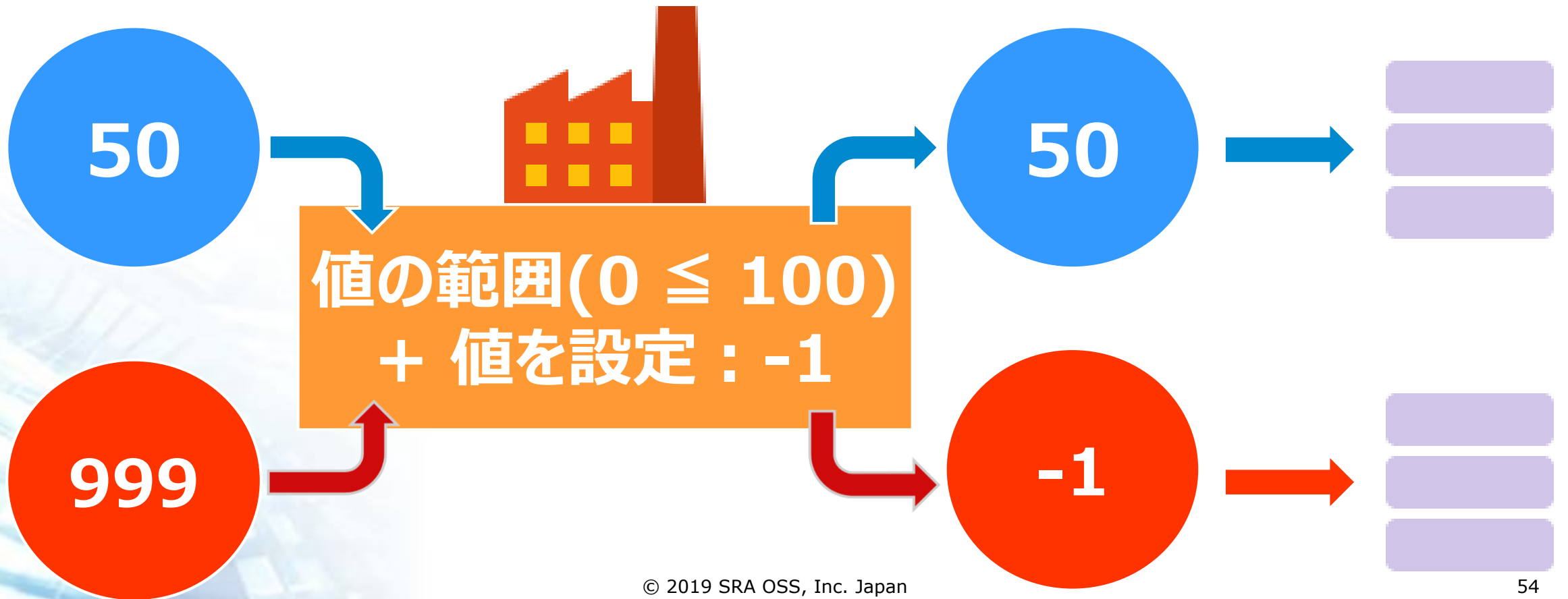
保存前処理の設定	名前	パラメータ	失敗時のカスタマイズ	アクション
1:	値の範囲	最小 最大	失敗時のカスタマイズ 値を破棄 値を設定 エラーを設定	☒ テスト 削除

保存前処理でエラーが発生しても
取得不可にしない

失敗時のカスタマイズ － 値を破棄 －

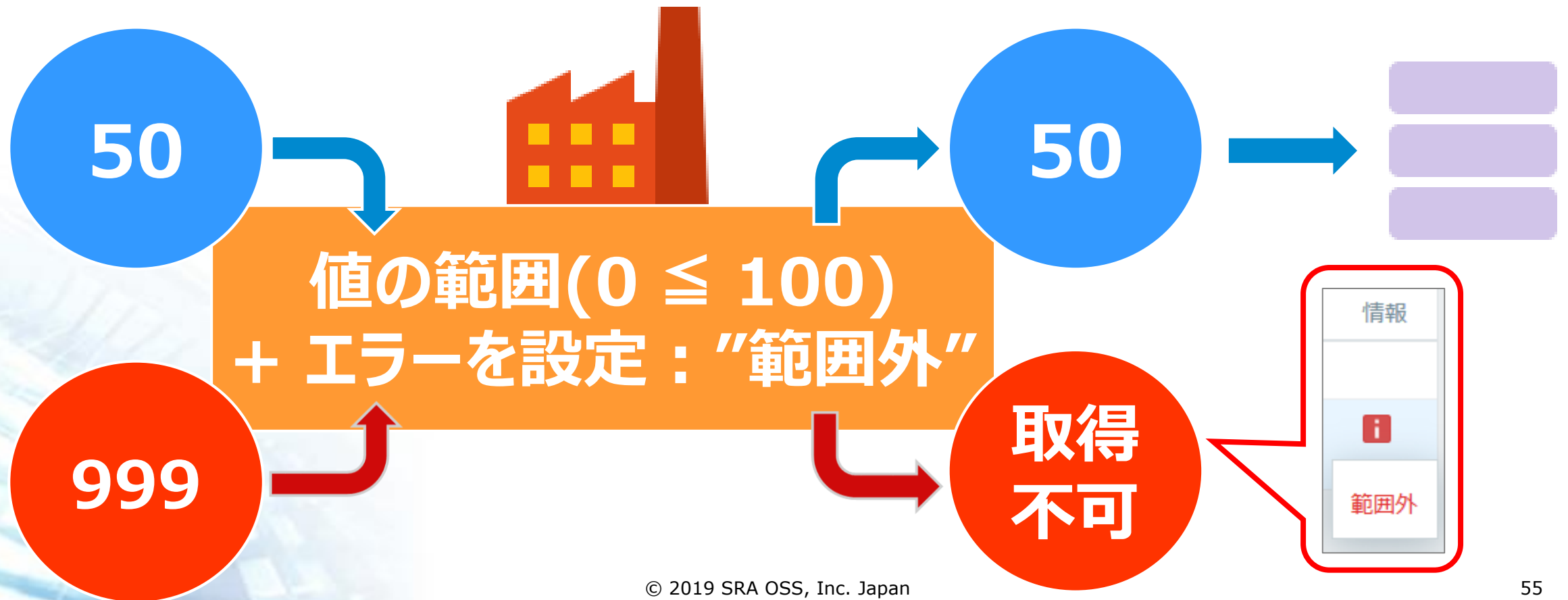


失敗時のカスタマイズ － 値を設定 －



失敗時のカスタマイズ

－エラーを設定－



JavaScript の失敗時のカスタマイズ

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: 追加	JavaScript	スクリプト	☐	テスト 削除 すべてのテスト

無効化されて選択できない

スクリプト内の if 文で同等の書き方が可能

- 値を破棄 ⇒ null を返す
- 値を設定 ⇒ 適当な値を返す
- エラーを設定 ⇒ 例外を投げる

保存前処理のテスト

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:	値の範囲	0	100	☐ テスト 削除
2:	乗数	5		☐ テスト 削除
追加				
更新 複製 監視データ取得 履歴とトレンドを削除 削除 キャンセル				

アイテム保存前処理テスト

値 50

時間 now

前の値

前の時間

End of line sequence

LF CRLF

保存前処理の設定

名前	結果
1: 値の範囲	50
2: 乗数	250

結果

Result converted to 数値 (整数)

250

テスト

キャンセル

エラー発生

結果

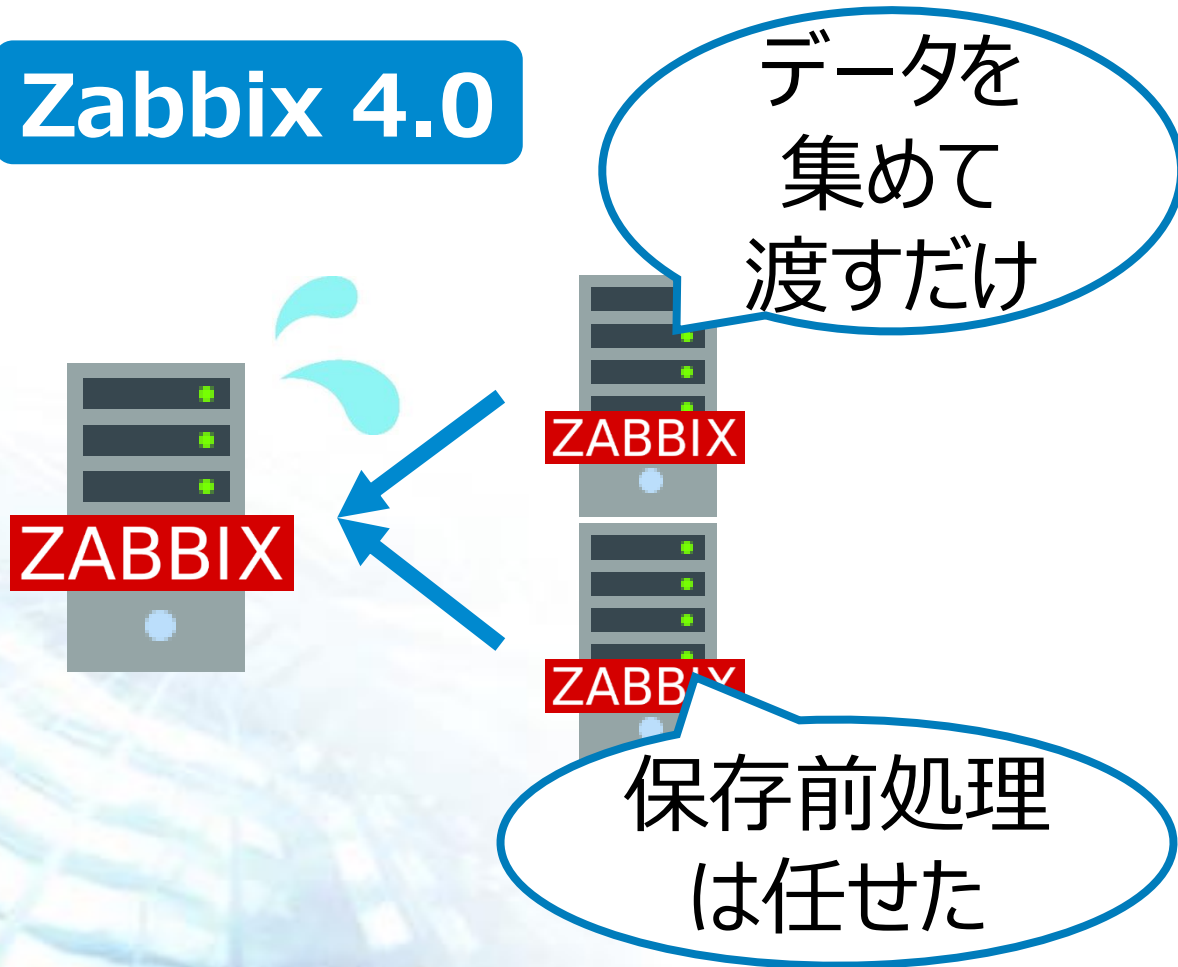
value is less than 0 or greater than 100

テスト

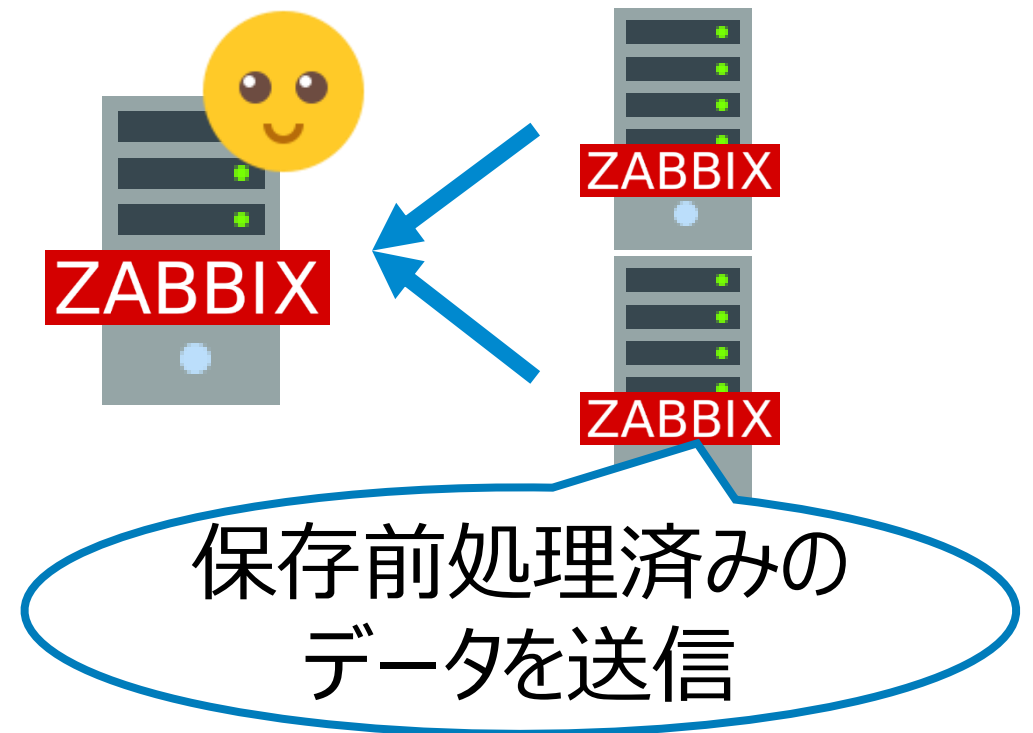
キャンセル

Zabbix proxy でのサポート

Zabbix 4.0

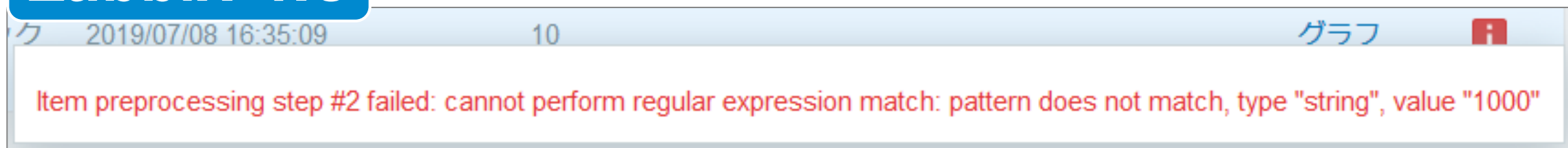


Zabbix 4.2

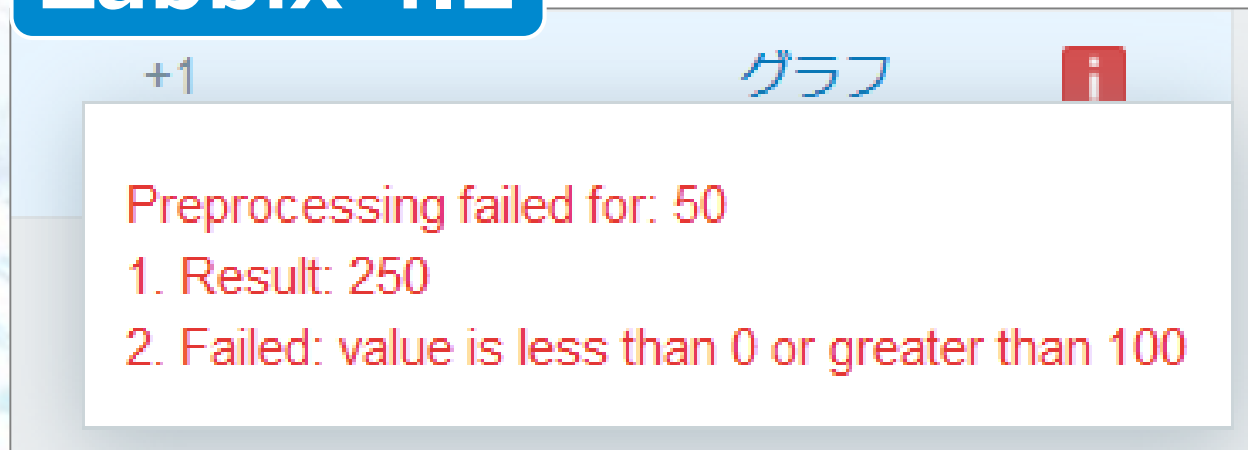


エラーメッセージの拡張

Zabbix 4.0



Zabbix 4.2



保存前処理の
どのステップで
エラーが発生したか
より分かりやすい



TimescaleDB サポート

- TimescaleDB とは
- TimescaleDB のアーキテクチャ
- housekeeper の違い



TimescaleDB とは



時系列データに強い PostgreSQL

PostgreSQL の EXTENSION

OSS

PostgreSQL
との互換性

パフォーマンス向上

データ削除が
速い

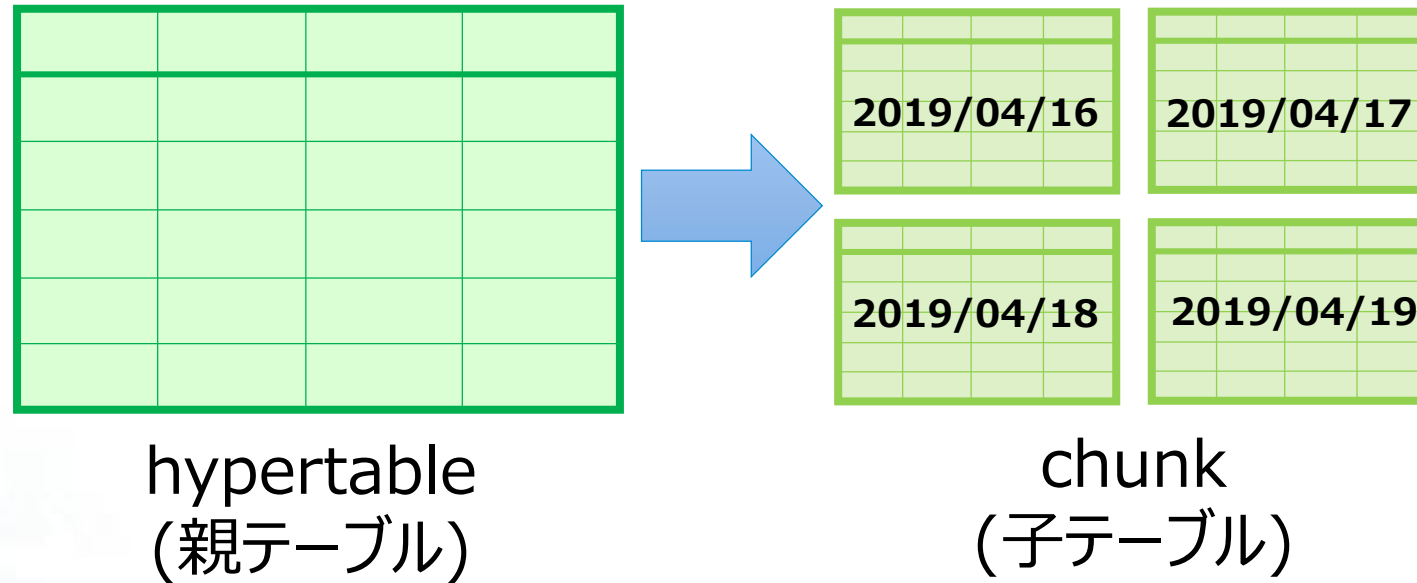
クエリも速い

時系列データ特化

時系列分析
関数

時系列データ
管理機能

TimescaleDB のアーキテクチャ

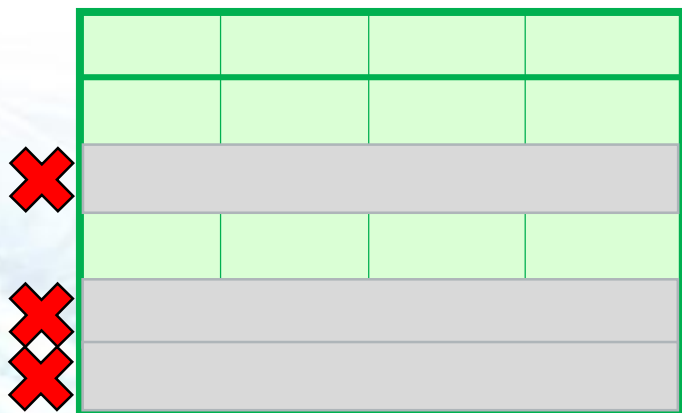


history テーブルを時間単位でパーティショニング

housekeeper の違い

PostgreSQL

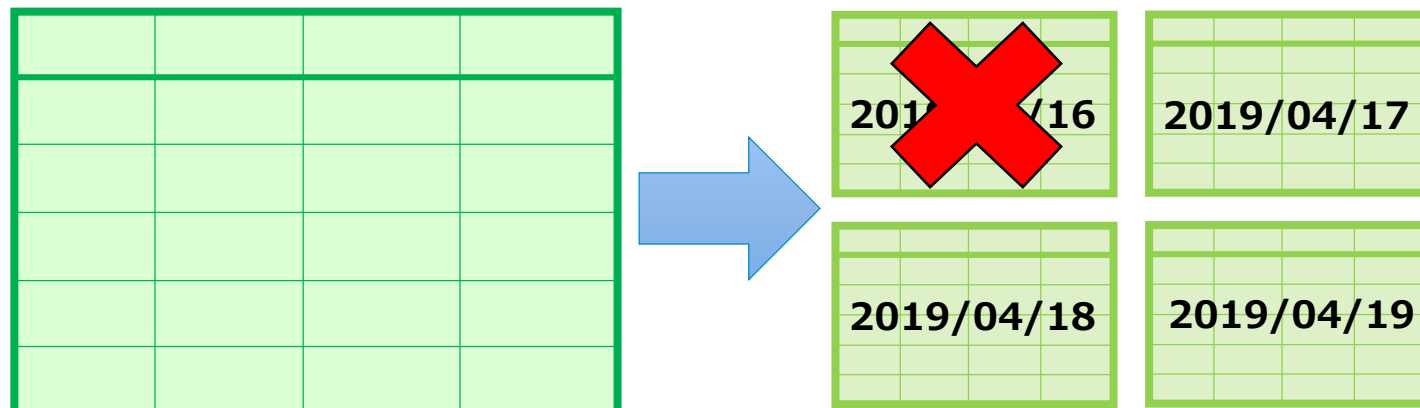
```
DELETE FROM history  
WHERE  
itemid = xxxx AND clock < yyyy
```



該当行を検索して削除
要 VACUUM

TimescaleDB

```
SELECT  
drop_chunks('history')
```



子テーブルごと削除
VACUUM 不要



ディスカバリの機能拡張

- ディスカバリによるホスト名の指定
- ローレベルディスカバリでの保存前処理
- JSONPath を使用した LLD マクロの追加
- その他のディスカバリの機能拡張

ディスカバリによるホスト名の指定

* チェック

Zabbixエージェント "system.uname" [変更](#) [削除](#)

SNMPv2エージェント "1.3.6.1.2.1.1.5.0" [変更](#) [削除](#)

[新規](#)

デバイスの固有性を特定する基準

☒ IPアドレス
 ☐ Zabbixエージェント "system.uname"
 ☐ SNMPv2エージェント "1.3.6.1.2.1.1.5.0"

ホスト名

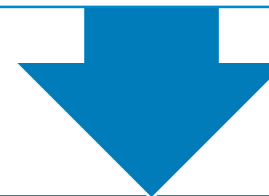
☒ DNS名
 ☐ IPアドレス
 ☐ Zabbixエージェント "system.uname"
 ☐ SNMPv2エージェント "1.3.6.1.2.1.1.5.0"

表示名

☒ ホスト名
 ☐ DNS名
 ☐ IPアドレス
 ☐ Zabbixエージェント "system.uname"
 ☐ SNMPv2エージェント "1.3.6.1.2.1.1.5.0"

Zabbix 4.0 まで

DNS or IP アドレス



Zabbix 4.2

チェック項目から指定

ローレベルディスクカバリでの保存前処理

[ディスクバリルール](#)
[保存前処理](#)
[LLDマクロ](#)
[フィルター](#)

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	パターン	出力	☐ テスト 削除
追加	テキスト			すべてのテスト
追加	正規表現			
	構造化データ			
	JSONPath			
	カスタムスクリプト			
	JavaScript			
	バリデーション			
	正規表現と一致しない			
	JSON内のエラーチェック			
	絞り込み			
	指定秒内に変化がなければ破棄			
	Prometheus			
	PrometheusからJSON			

JSONPath を使用した LLD マクロの追加

前処理	LLDマクロ	フィルター
	LLDマクロ	JSONPath
	{#NAME}	\$.name 削除
	{#FSNAME}	\$.fs.name 削除

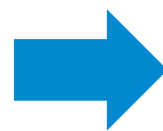
```
{  
  "name": "/dev/sda1",  
  "fs": {"name": "xfs", }  
}
```

```
{  
  "{#NAME}": "/dev/sda1",  
  "{#FSNAME}": "xfs",  
}
```

その他のディスカバリの機能拡張

- LLD ルールを通常アイテムの依存アイテムとして設定可能
- LLD ルールを処理するプロセスが独立したプロセスに
- LLD ルールが受け入れる JSON フォーマットが変更

```
{  
  "data": [  
    {discovery row},  
    {discovery row}  
  ]  
}
```



```
[  
  {discovery row},  
  {discovery row}  
]
```



Prometheus との統合

Prometheus との統合

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:	Prometheusパターン	<メトリクス名>{<ラベル名>="ラベル値", <ラベル名>}	☐	テスト 削除
2:	PrometheusからJSON	<メトリクス名>{<ラベル名>="ラベル値", ...} == <値>	☐	テスト 削除

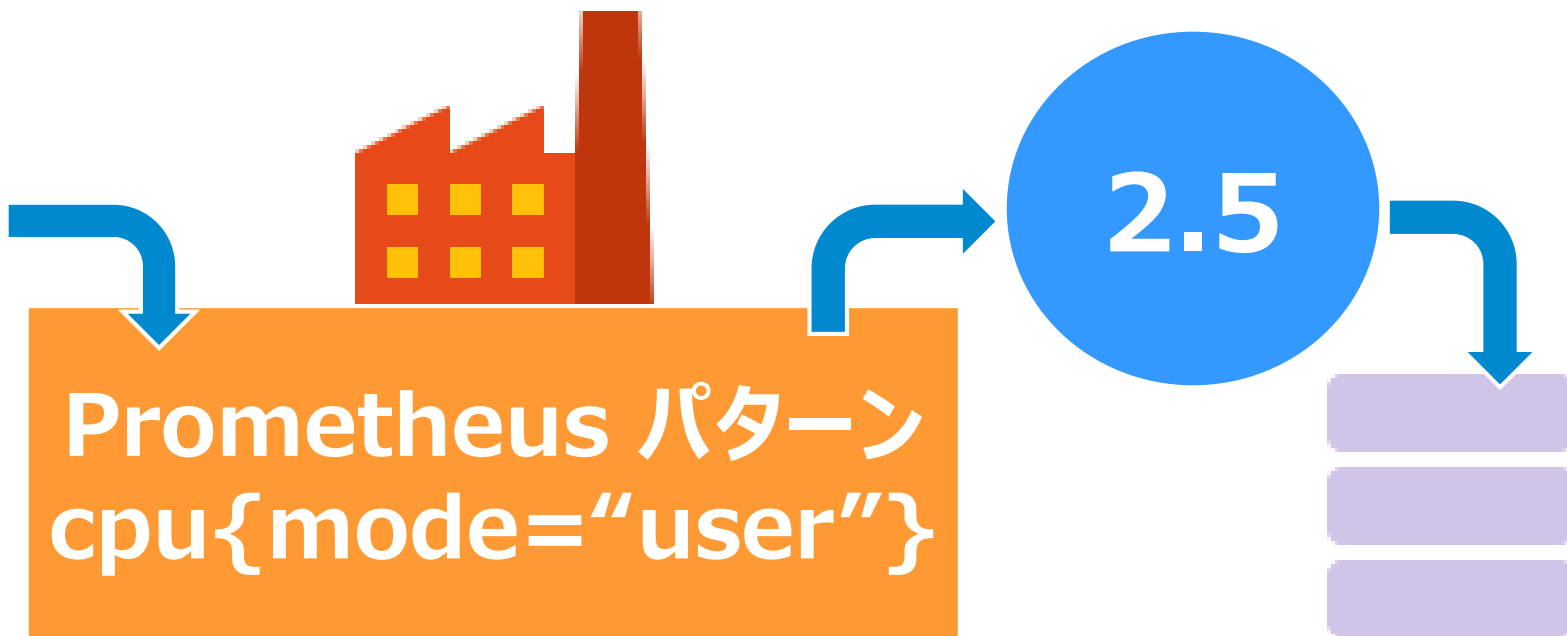


メトリクス名{ラベル名="ラベル値",...} メトリクス値

Prometheus との統合

– Prometheus パターン –

```
cpu{mode="sys"} 0.2  
cpu{mode="user"} 2.5  
cpu{mode="idle"} 95.2
```

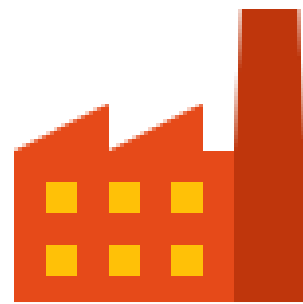


Prometheus パターンからメトリクスを抽出

Prometheus との統合

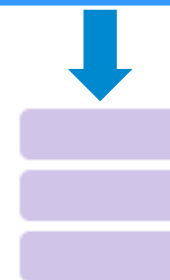
– Prometheus から JSON –

`cpu{mode="sys"} 0.2`
`cpu{mode="user"} 2.5`
`cpu{mode="idle"} 95.2`



```
[{  
  "name": "cpu",  
  "value": "0.2",  
  "line_raw": "cpu{cpu=mode=¥\"sys¥\"} 0.2¥r",  
  "labels": {"mode": "sys"},  
}]
```

Prometheus から JSON
`cpu{mode="sys"}`



Prometheus ⇒ JSON ⇒ LLD マクロ ⇒ LLD ルール



通知・メディアの機能拡張

- E メール通知での HTML フォーマットサポート
- メディアタイプのテスト

Eメール通知での HTML フォーマットサポート

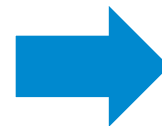
* 送信元メールアドレス

接続セキュリティ

認証

メッセージフォーマット

有効 ☒



デフォルトのメッセージ

```
<html>
<head>
<style type="text/css">
#Warning {color: #FFC859}
</style>
</head>
<body>
<h1>障害詳細</h1>
<ul>
<li>日時: {EVENT.DATE} {EVENT.TIME}</li>
<li>障害: {EVENT.NAME}</li>
<li>ホスト: {HOST.NAME}</li>
<li>深刻度: <span id="{EVENT.SEVERITY}">{EVENT.SEVERITY}</span></li>
<li>イベント ID: {EVENT.ID}</li>
</ul>
<a href="{TRIGGER.URL}">トリガー詳細</a><br>
</body>
</html>
```

障害詳細

- 日時: 2019.07.08 12:48:59
- 障害: test
- ホスト: test
- 深刻度: Warning
- イベント ID: 1427

トリガー詳細

メディアタイプのテスト

メディアタイプの作成

フィルター 

アクション

テスト
テスト
テスト
テスト



メディアタイプのテスト

✓ メディアタイプのテストに成功しました。

* 送信先

件名

* メッセージ

テスト キャンセル



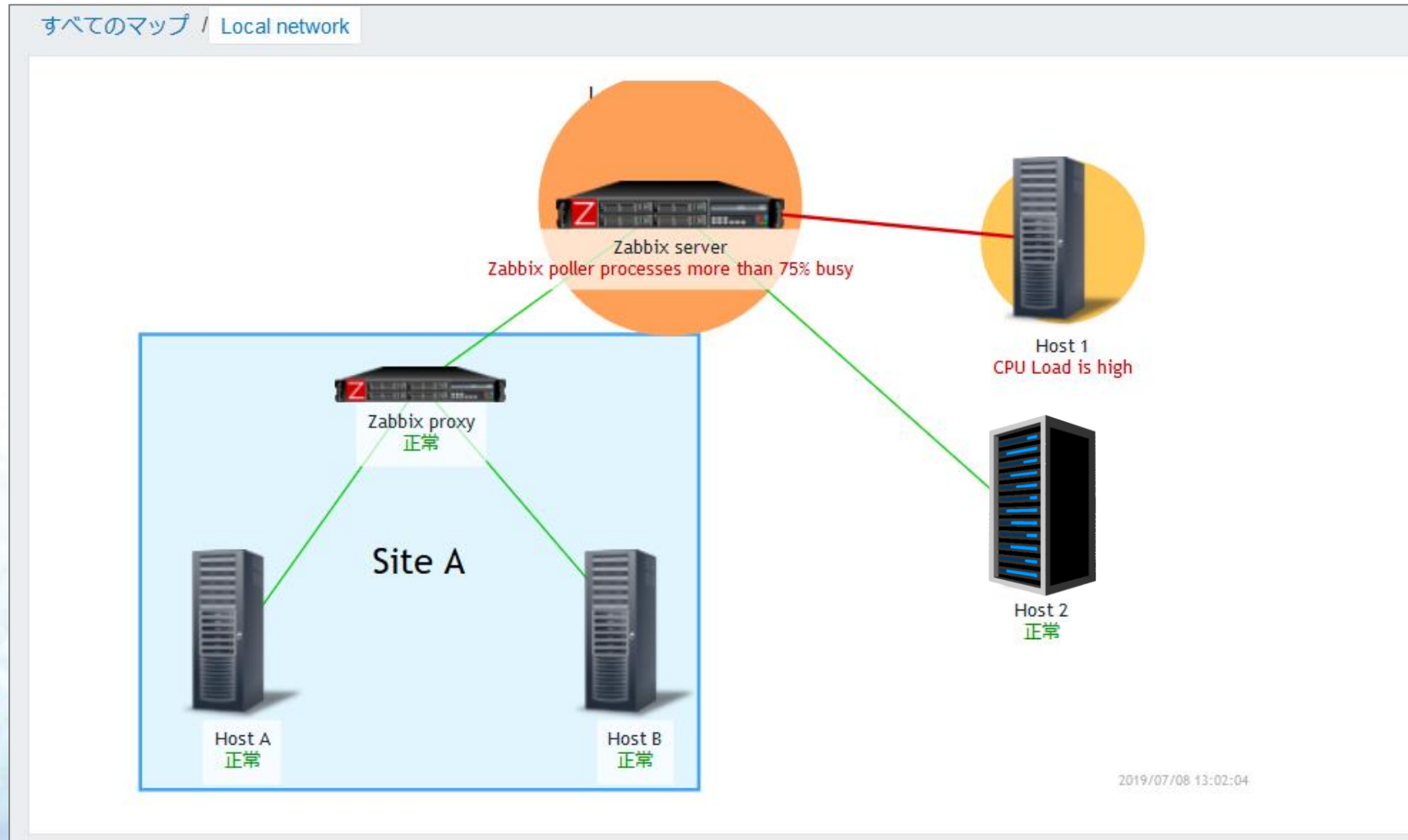
マップの機能拡張

- マップで使用可能なマクロの追加
- マップでのアニメーション GIF サポート

マップで使用可能なマクロの追加

場所	ホスト要素	ホストグループ要素	トリガー要素	マップ要素
ラベル	{HOST.ID} {INVENTORY.*}	{HOSTGROUP.ID} {INVENTORY.*}	{TRIGGER.ID} {INVENTORY.*}	{MAP.ID} {MAP.NAME}
URL の名前	{HOST.ID}	{HOSTGROUP.ID}	{TRIGGER.ID}	{MAP.ID}
URL の名前および値	{HOST.CONN/ DNS/HOST/IP/ NAME} {INVENTORY.*}	{HOST.CONN/ DNS/HOST/IP/ NAME} {INVENTORY.*}	{HOST.CONN/ DNS/HOST/IP/ NAME} {INVENTORY.*}	{MAP.NAME}

マップでのアニメーション GIF サポート



フロントエンドの機能拡張

- トリガー一覧画面のフィルタ項目追加
- SVG のツールチップにタイムスタンプ表示

トリガー一覧画面のフィルタ項目追加

トリガー

グループ: すべて ▼ ホスト: Zabbix server ▼ トリガーの作成

すべてのホスト / Zabbix server 有効 ZBX SNMP JMX IPMI アプリケーション 14 アイテム 105 トリガー 57 グラフ 20 ディスカバリールール 2 Webシナリオ フィルター

深さ: すべて 未分類 情報 警告 軽度の障害 重度の障害 致命的な障害 タグ: And/Or Or

状態: すべて ノーマル 不明

ステータス: すべて 有効 無効

値: すべて 正常 障害

タグ: タグ 含む 等しい 値 削除

追加

適用 リセット



トリガー

すべてのホスト / Zabbix server 有効 ZBX SNMP JMX IPMI アプリケーション 12 アイテム 100 トリガー 52 グラフ 17 ディスカバリールール 3 Webシナリオ フィルター

トリガーの作成

ホストグループ: 検索文字列を入力 選択

ホスト: Zabbix server ✕ 検索文字列を入力 選択

名前:

深さ: ☐ 未分類 ☐ 情報 ☐ 警告 ☐ 軽度の障害 ☐ 重度の障害 ☐ 致命的な障害

状態: すべて ノーマル 不明

ステータス: すべて 有効 無効

値: すべて 正常 障害

タグ: And/Or Or

タグ: タグ 含む 等しい 値 削除

追加

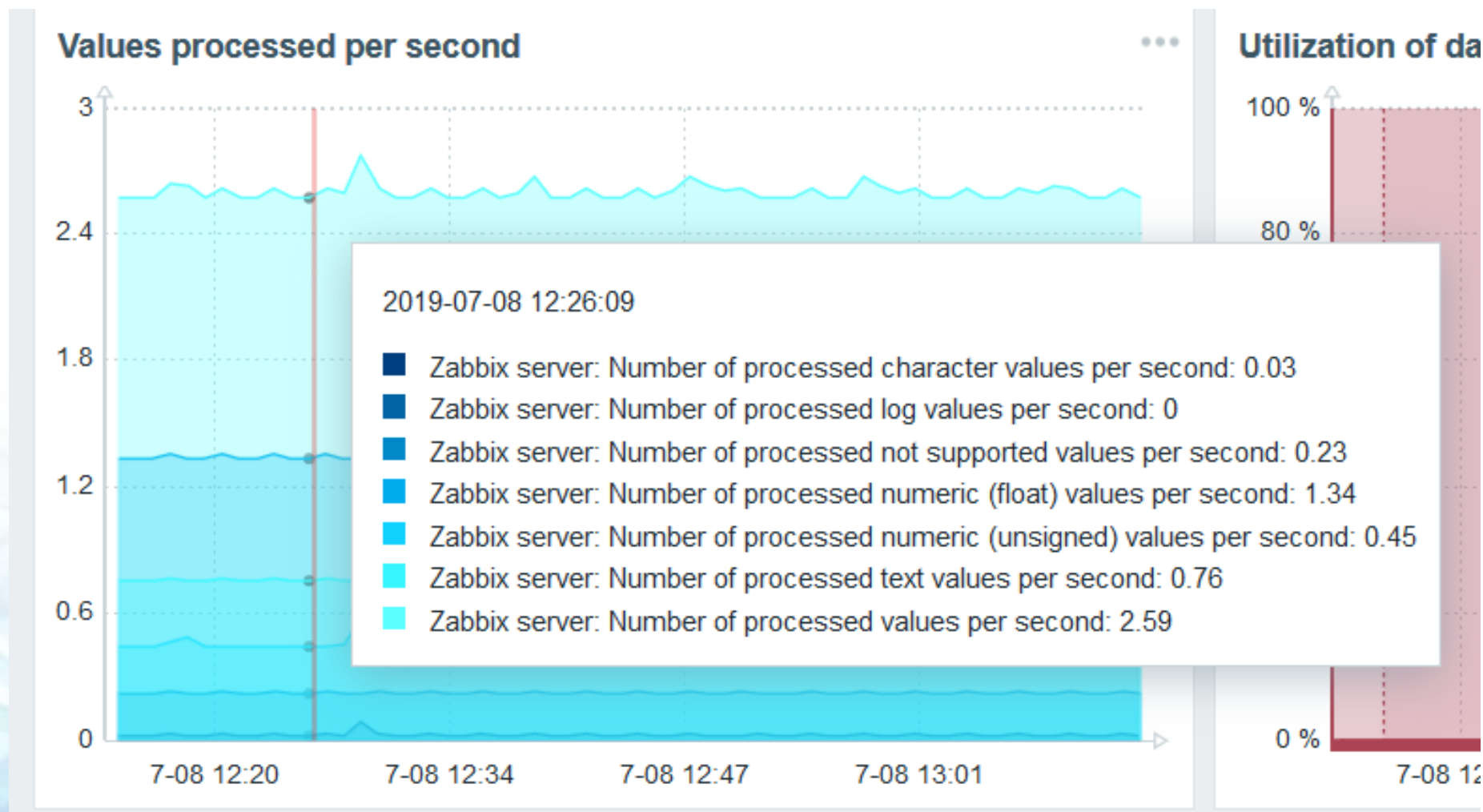
継承したもの: すべて はい いいえ

Discovered: すべて はい いいえ

依存関係がある: すべて はい いいえ

適用 リセット

SVG のツールチップにタイムスタンプ表示





その他

その他の機能拡張

- Web 監視で HTTP ヘッダ内を正規表現で検索可能に
- zabbix_sender が ServerActive で設定した全 IP アドレスにデータ送信可能に
- ダッシュボードウィジェットの非破壊リサイズ/並べ替え
- アイテムプロトタイプの一括更新
- net.dns、net.dns.record で IPv6 をサポート
- vmware.eventlog に skip パラメータ追加



Zabbix 4.4 について

- テンプレート
- シンタックスの統一
- プラグイン
- ベースライン監視

テンプレート

- テンプレート作成のガイドライン
- テンプレートのバージョンニング
- テンプレートを XML 形式から JSON/YAML 形式に

```
<templates>
  <template>
    <template>Template name</template>
    <name>Template name</name>
    <description/>
    ...
```



```
templates:
  template:
    template: "Template name"
    name: "Template name"
    description:
    ...
```

シンタックスの統一

func(param1, param2, param3, ...)

・トリガー

{host:key.func(param)}op const

・計算アイテム

func(key|host:key, param1, ...)

・アグリゲート

grpfunc[group, key, func, period]



・トリガー

func(host:key, param)op const

・計算アイテム

func(key|host:key, param1, ...)

・アグリゲート

grpfunc(group, key, func, period)

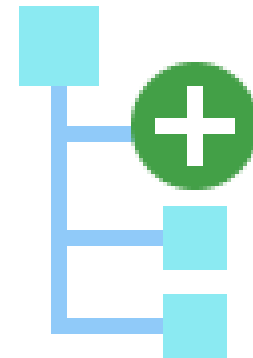
プラグイン

- **Webhook**

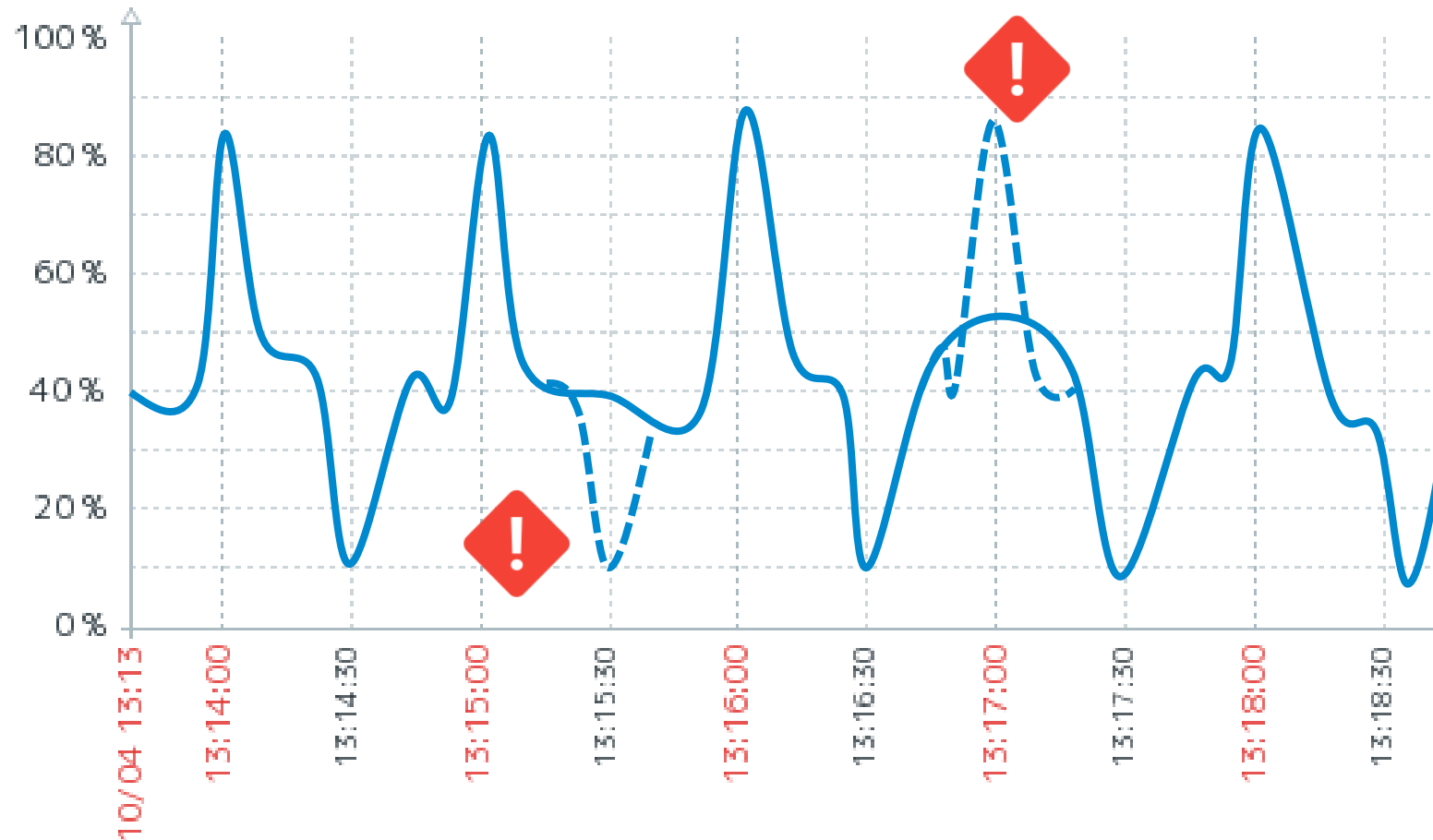
- アクション実行時の Webhook
- 障害発生時の Webhook



- トップレベルおよびコンテキストメニューへの
独自リンクの追加

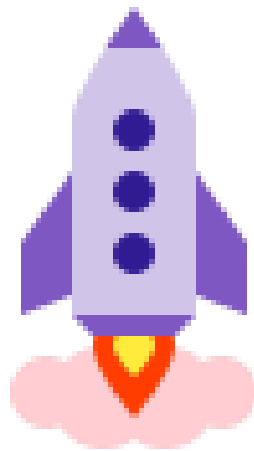


ベースライン監視



Zabbix 4.4 リリース予定

2019 年 9 月





ZABBIX で
効率的な監視運用を！

