

北海道自治体向けクラウドサービスでのZabbix導入事例とOSS連携のご紹介

平成29年11月17日

株式会社

HARP

自己紹介

- 外崎 幸大
- 北海道 富良野出身
- ネットワークエンジニア
- 子どもは3人います
- 最近の趣味はInstagramと革細工



プロジェクト推進部
IT基盤グループ

外崎 幸大
yukihiko sotozaki

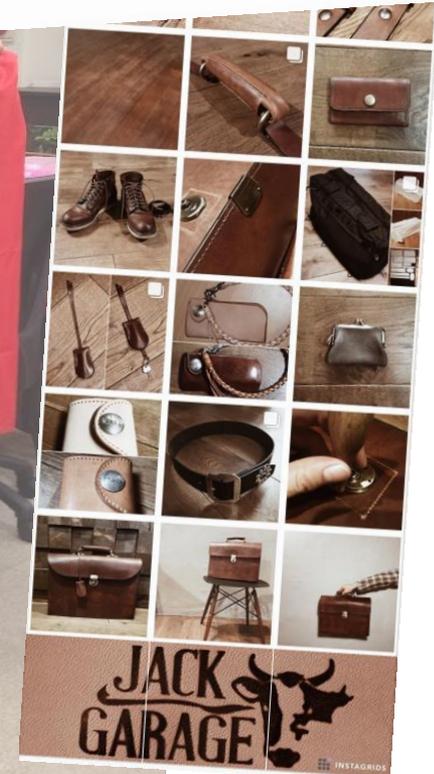


HARP

ZABBIX
CERTIFIED PROFESSIONAL

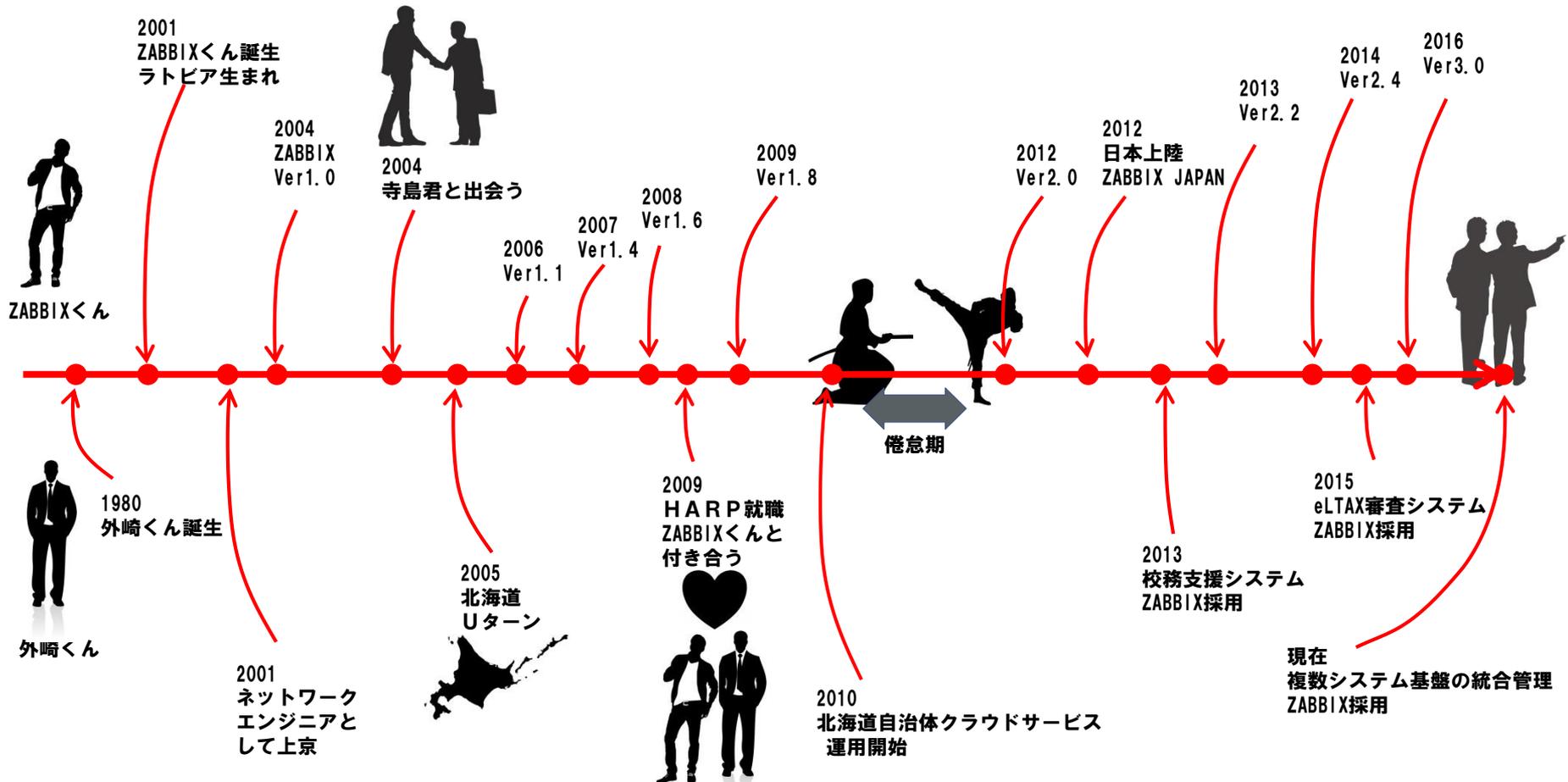
株式会社 HARP

〒060-0001
札幌市中央区北1条西6丁目1-2アーバンネット札幌ビル3F
TEL:011-221-5800 FAX:011-212-7082
E-mail:yukihiko.sotozaki@e-harp.jp
URL:http://www.e-harp.jp



自己紹介

ZABBIXと私の思い出年表



会社概要

項目	内容
商号	株式会社HARP
本店所在地	札幌市中央区北1条西6丁目1-2 アーバンネット札幌ビル3階
設立	平成16年9月21日
資本金	資本金 471,000千円
主な出資者	・北海道 ・NTT東日本 ・北海道電力グループ ・北洋銀行グループ ・北海道ガス
事業内容	<ul style="list-style-type: none">・情報システムの企画、設計及び管理運営・情報収集・処理の提供サービス・コンピュータシステム構築のコンサルティング業務・コンピュータソフトウェア・ハードウェアの開発、販売・システムインテグレーション（総合的なコンピュータシステムの構築及び保守）業務・コンピュータシステム構築の教育又はプログラムの設計技術者の派遣・前各号に付帯する一切の業務
セキュリティ 認証等	<ul style="list-style-type: none">・平成18年2月10日、ISMS認証基準（Ver.2.0）認証取得・平成18年2月21日、プライバシーマーク認定取得

Zabbix導入前（運用環境の課題）

導入前の課題



サービス毎に監視ツールが導入され管理が煩雑

The Webalizer
What is your web server doing today?

有人監視オペレータの監視レベルにばらつきがある

一元的な監視ができず、障害の特定に時間がかかる

Tivoli

MRTG
MULTI ROUTER TRAFFIC GRAPHER



監視システム導入の選定方針

監視ツールを統一

監視水準の統一

監視運用の効率化

ZABBIX

なぜZabbixを採用したのか

- OSS積極活用しコスト減の取り組み

- トライ＆エラーが許される状況だった

- 特定のベンダーに依らない自治体主導の電子自治体の提供

- コミュニティの活発さと、寺島君の友情サポート

Zabbix導入後の課題①

課題・・・監視マップの作りこみが大変

困っていた運用オペレーション

- ・ ホスト種別分のアイコンを作る・探して見繕う
- ・ 正常・異常要アイコンを登録する
- ・ マップのインポートもエクスポートもできない

The screenshot displays the Zabbix 2.2.9 web interface. On the left, the 'Network Map Configuration' window is open, showing a map titled 'Local network' with a grid and a host icon (server) placed on it. The host is labeled 'Zabbix server' with IP '127.0.0.1'. On the right, the 'Host Configuration' window is open, showing the 'Selected Hosts' list with 'Server_96' selected. Below this, there are various configuration options like 'Label', 'Label position', 'Automatic icon selection', and 'Icon selection'. The 'Icon selection' section shows a list of icons for different host types, including 'Crypto-router', 'Disk array 3D', and 'ellex_error'. The 'ellex_error' icon is highlighted, indicating it is selected for the host.

困っていた運用オペレーション

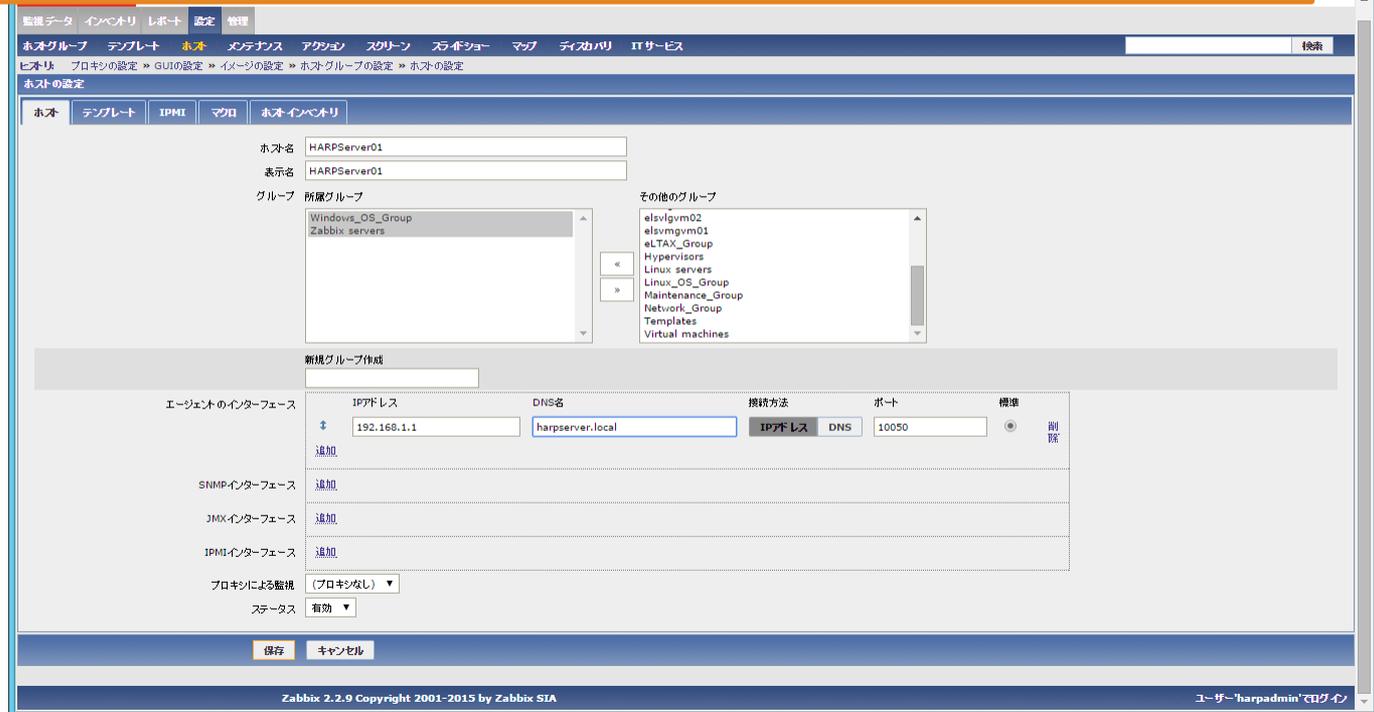
- ・ ネットワーク毎のマップにホストの台数分を登録
- ・ ホスト毎の接続性を手動で設定
- ・ ステータス事に表示させたいアイコン設定
- ・ 保存ボタン押し忘れて1から作成しなおし・・・

Zabbix導入後の課題②

課題・・・監視ホストの登録が手動登録大変

困っていた運用オペレーション

- ・ 表示名やホスト名、アドレス情報等を手入力
- ・ 対象ホストの数分繰り返し登録作業が必要
- ・ 監視テンプレートはあるが、適用作業もそれなりに大変

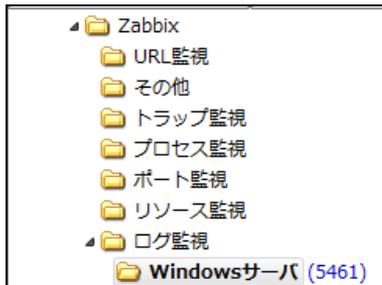


Zabbix導入後の課題③

課題・・・監視登録直後にWindowsのイベントログアラートが大量に通知

困っていた運用オペレーション

- ・WINDOWSイベントログ監視で「WARNING」は全部トリガ
- ・トリガされたイベントで警告異常はメール通知
- ・金曜日監視テンプレをWINDOWSグループ全体に適用して帰社
- ・月曜日出社すると、アラートメールが数千通・・・



件名	差出人	送信日時
[] [_ml:3334] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3335] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3332] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3330] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3329] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3328] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3326] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3325] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		
[] [_ml:3327] ログ監視状況(sys):i .local[]:PROBLEM Zabbix 障害通知 <zabbix@ >		

差出人: Zabbix 障害通知 <zabbix@	宛先: []:PROBLEM	日時:
件名: []_ml:3334] ログ監視状況(sys):i .local[]:PROBLEM		

このメールはZABBIX : 通称【そとにゃん】が送信している監視通知メールです。

localのログ監視状況(sys)で問題を発見しました。

発生日時:
 重要度: Warning
 イベントID: 16
 ログソース: Microsoft-Windows-WindowsUpdateClient
 OS種別: Windows

ログの詳細を確認するには、.local[]にログインし、イベントビューアにて確認して下さい。

課題の原因

初回の監視はログ行頭からチェック→1行目から最終行までをチェック
 結果、過去数か月分のログ内容から、全WARNINGを通知することに

Zabbix導入後の課題④

課題・・・トラップやログ監視で短期間に複数の障害を検知すると誤検知

監視取得値

```
jul 18 13:00:29 host01 kernel: xxx: error=1234  
jul 18 13:00:29 host01 kernel: xxx: error=5678
```

検知条件

```
log[/var/log/messages,error | Error]
```

アクション メール通知

{EVENT.TIME}に{HOST.NAME1}の{ITEM.NAME1}で障害が発生しています。
監視取得値：{ITEM.VALUE1}

困っていた監視結果

2通のメール通知、監視取得値の内容が違う

1通目

13:00:29にhost01のメッセージログ監視で障害が発生しています。
監視取得値：kernel: xxx: error=5678

2通目

13:00:29にhost01のメッセージログ監視で障害が発生しています。
監視取得値：kernel: xxx: error=5678

課題の原因

メッセージの取得精度の問題で、ログデータをメールのメッセージ内に
取りこめない場合があった

Zabbix導入後の課題⑤

課題・・・クライアント証明書対応のWEBページ監視ができない

シナリオ **ステップ**

認証タブがない

フォーラムで聞く
Web監視の機能でなんとかできないか・・・
Curlが裏で動いてるらしいことを知る

名前

リケーション

リソースの作成

認証 なし

更新間隔(秒)

リトライ

エージェント Internet Explorer 10.0

HTTPプロキシ http://[username[:password]@]pr

変数

有効

日本Zabbixユーザー会
Japanese Zabbix Community

ログアウト アカウント設定 RSS

HOME NEWS FORUM DOCUMENTS DEMO CONTACT

ikemoさんについて

アカウント名 ikemo
ユーザープロフィールを表示

クライアント証明書が必要なWEB監視

2013/01/31 - 18:03 (木) ikemo - 投稿数: 41 日本Zabbixユーザー会フォーラム

クライアント証明書が必要なWebページの監視を行いたいのですが、zabbixのWeb監視機能からはクライアント証明書指定できないため、CURLの環境変数にクライアント証明書を指定し、強制的にクライアント証明書を使用させるようにして、うまく監視ができません。
error doing curl_easy_perform: SSL connect error
となっています。

curlコマンドで直接実行すると環境変数を見に行っても正しい結果が返ってくるのですが、zabbixでは環境変数を見に行ってくれないのでしょうか。

PHPファイルのどこかに記述があるのでしようが、プログラミングに疎く、皆様のご協力をいただけると助かります。

< ログイン出来ない EUC形式のログ監視について >

困っていた運用オペレーション
ユーザーパラメータを使用して乗り切る

```
web.check[*],curl -L -i --connect-timeout 15 --cert xxxcert.pem --key xxxkey.pem $1
| egrep "$2" | wc -l
```

Zabbix導入後の課題は勝手に解決！

監視マップの作りこみ

ZABBIX
Ver2.0

アイコン自動マッピング
ホストグループ内ホスト登録

監視ホストが手動登録

ZABBIX
Ver2.2

アクティブAgent自動登録

ログ監視アラートが大量通知

ZABBIX
Ver2.0

Eventlogアイテムにmodeパラメータ登場

短期間での複数障害で誤検知

ZABBIX
Ver2.0

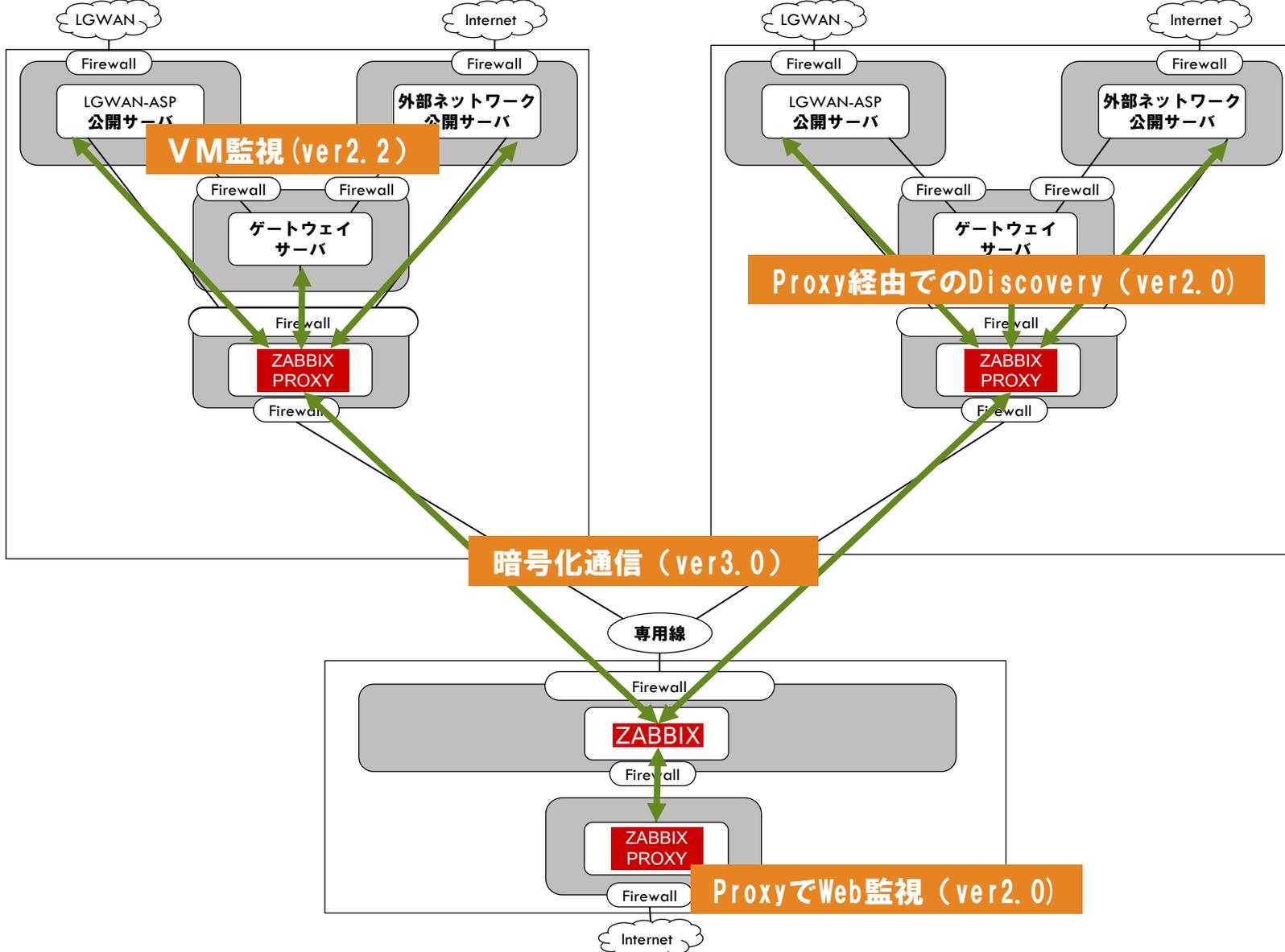
監視値の取得精度がナノ秒対応

URL監視がクライアント証明書非対応

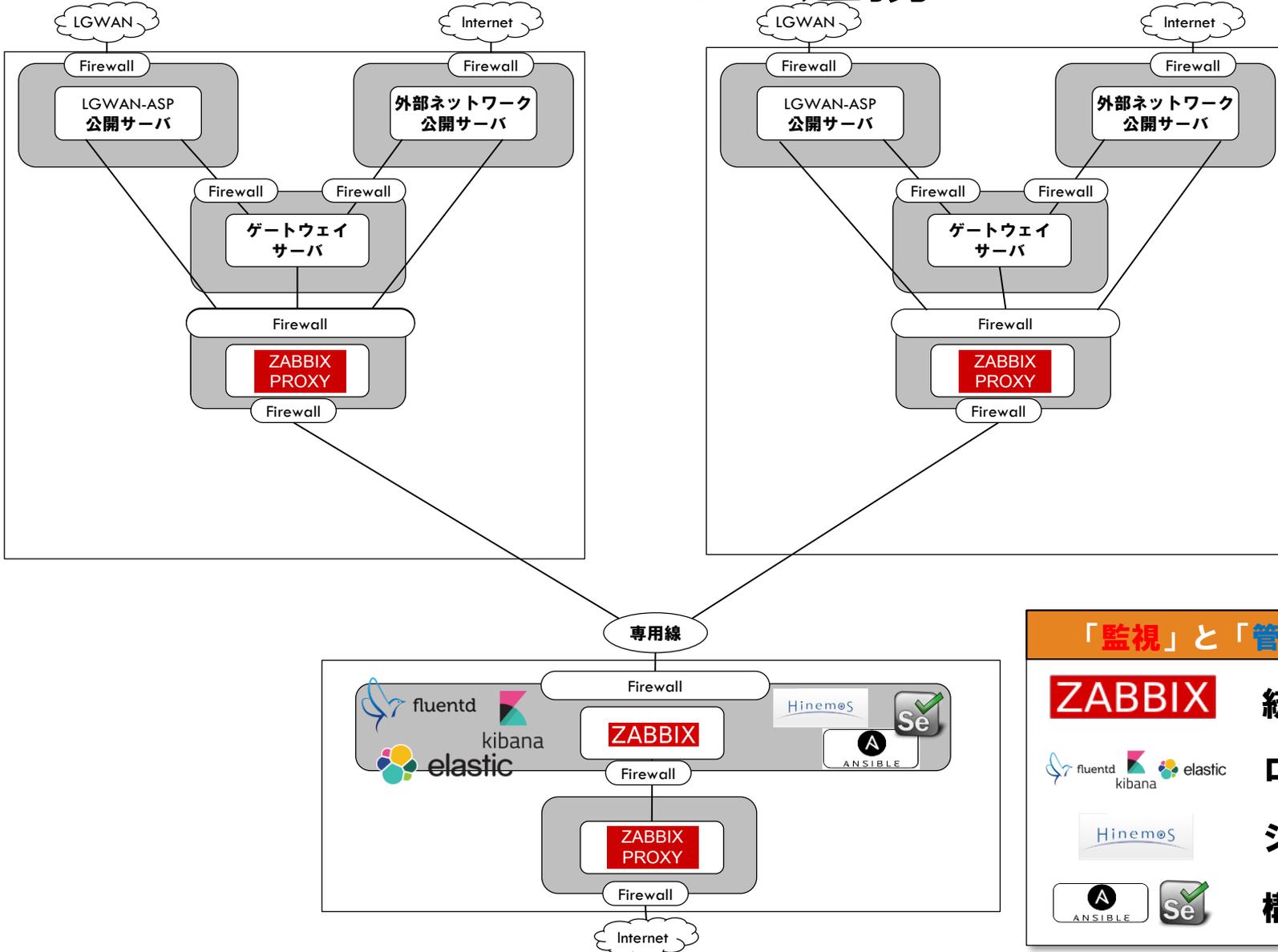
ZABBIX
Ver2.4

クライアント証明書対応

北海道自治体クラウドサービスとZabbix運用環境



ZabbixとOSSとの連携について

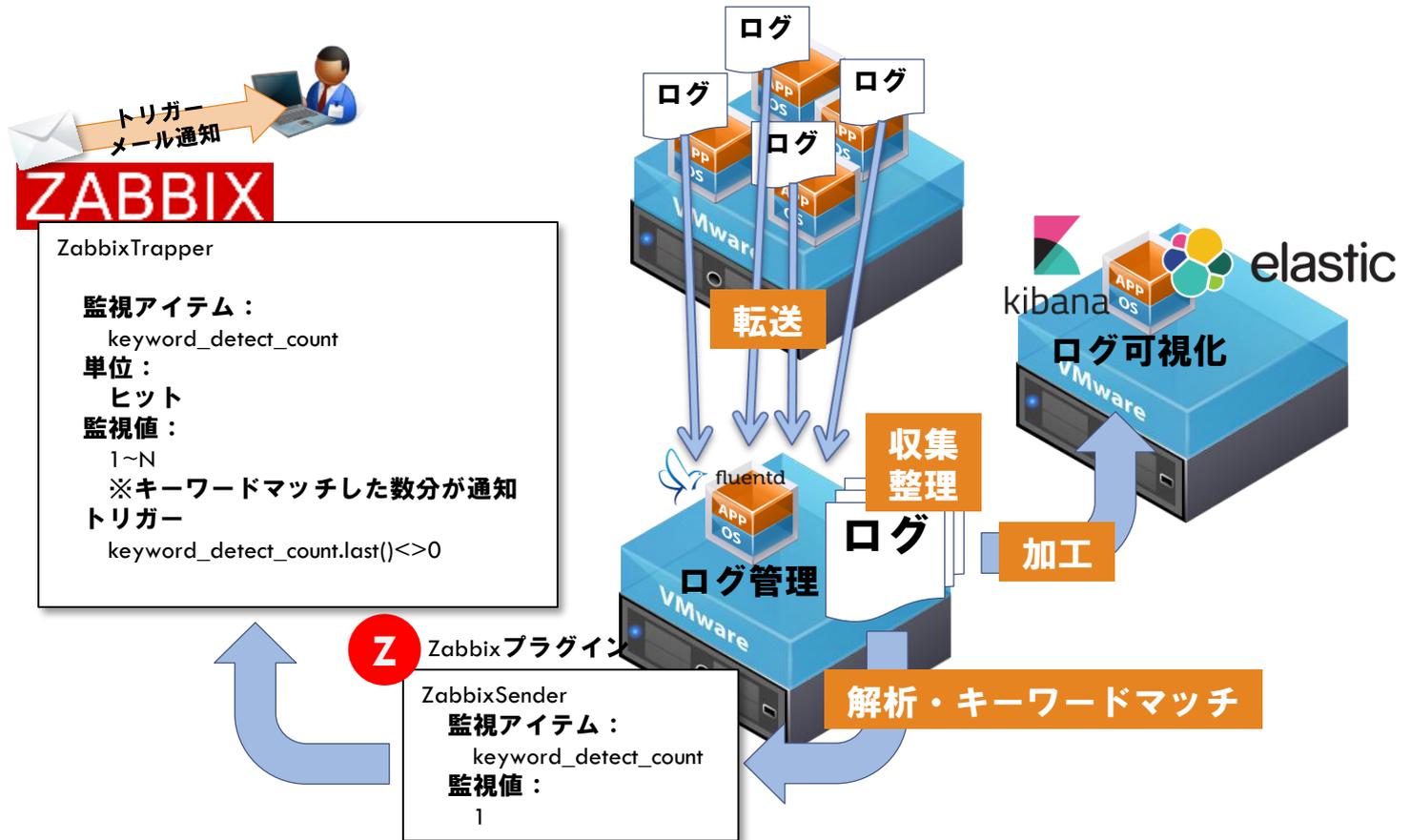


「監視」と「管理」を区別

	統合監視
	ログ管理
	ジョブ管理
	構成管理

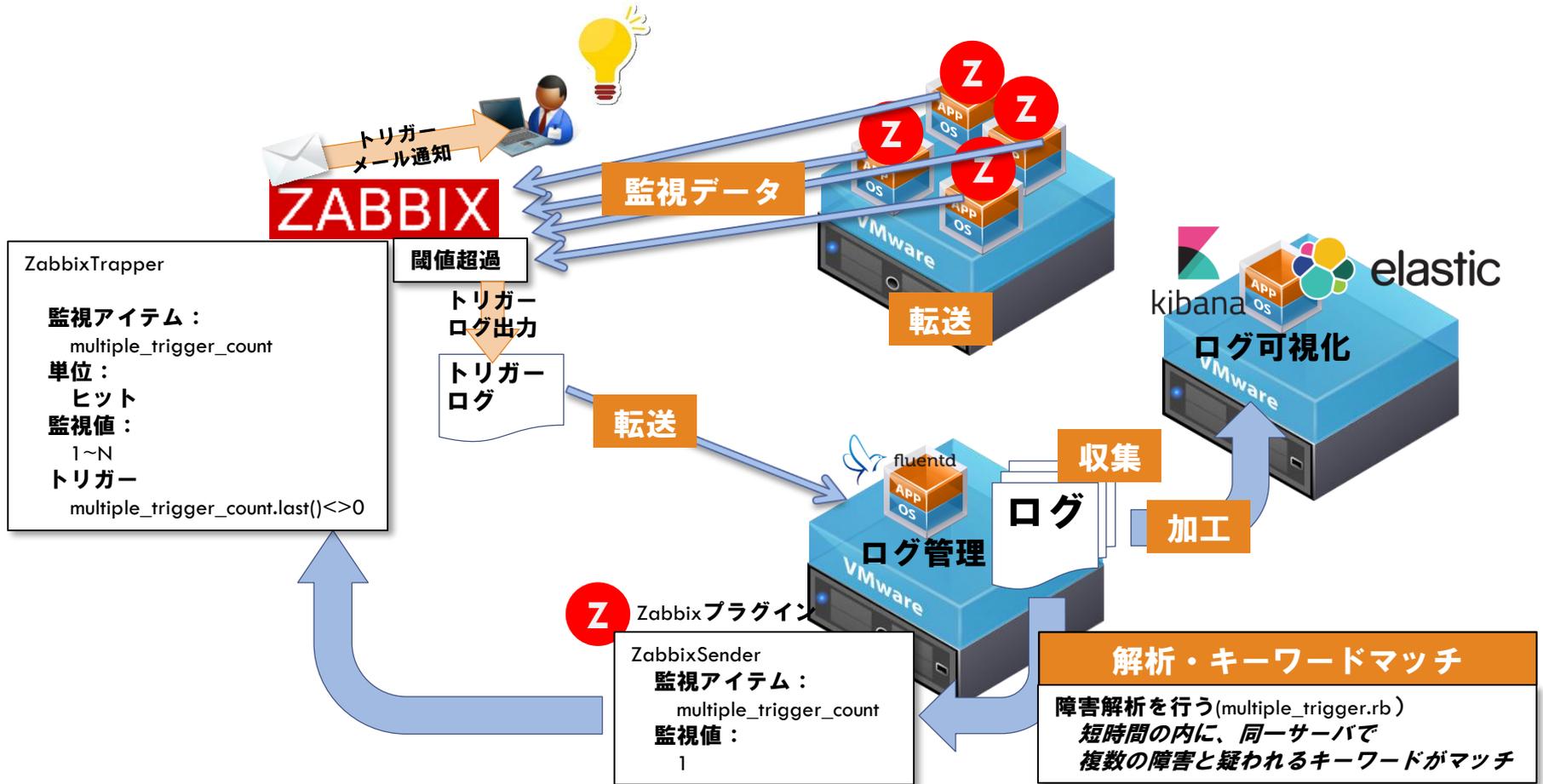
Zabbix + fluentd + kibana + elasticsearch

ログ収集はFluentdで実施し、情報の整理はKibanaとelasticsearchが担当
 収集ログの解析はFluentdで行い、解析結果をZabbixに送信



Zabbix + fluentd + kibana + elasticsearch

ログ解析が得意なFluentdと連携する事で、高度な監視を実現



Zabbixの良いところ（私見）

他システムの連携性

OSSの性質上、仕様が公開されていることもあり、他システムとの連携に関する情報が広く普及している

サポートが充実

質の高いコミュニティが活発（日本Zabbixユーザ会）

実装レベルで解決可能な有用な情報が満載

リリース計画

ニーズに遅れる事なくリリース対応
計画されたリリース対応が将来に安心感

ノウハウの蓄積

統合監視ツールは多機能な反面、ノウハウの習得が大変

監視テンプレートという形でノウハウが残せる

アップグレードでも操作方法は変わらない

今後に期待すること

テンプレートやディスカバリ等一括で追加された監視アイテムに対する変更が苦手

ZABBIX

Ver ?

WindowsOSコマンド実行結果をエンコード

ZABBIX

Ver ?

Web監視のSSLピア検証でメモリリーク

ZABBIX

Ver ?

ZabbixProxyの成長

ZABBIX

Ver ?

いつ頃かな？